CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES INSTITUTO FEDERAL DE SANTA CATARINA

LIAMARI DE ARAÚJO

ESTUDO DE APLICAÇÕES DAS TÉCNICAS DE ACESSO IP-VPN EM LABORATÓRIOS DE INFORMÁTICA DO PROINFO NAS ESCOLAS DA GRANDE FLORIANÓPOLIS

São José, SC

2014

LIAMARI DE ARAÚJO

ESTUDO DE APLICAÇÕES DAS TÉCNICAS DE ACESSO IP-VPN EM LABORATÓRIOS DE INFORMÁTICA DO PROINFO NAS ESCOLAS DA GRANDE FLORIANÓPOLIS

Proposta de TCC2 apresentada à Coordenação do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal de Santa Catarina para a obtenção do diploma de Tecnólogo em Sistemas de Telecomunicações.

Orientador: Prof. Alexandre Moreira, M.
Co-Orientadora: Profª. Claudinice Carla Bertotti

São José, SC

2014

LIAMARI DE ARAÚJO

ESTUDO DE APLICAÇÕES DAS TÉCNICAS DE ACESSO IP-VPN EM LABORATÓRIOS DE INFORMÁTICA DO PROINFO NAS ESCOLAS DA GRANDE FLORIANÓPOLIS

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Tecnólogo em Sistemas de Comunicações e aprovado em sua forma final pelo Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal de Santa Catarina.

Florianópolis, Dezembro de 2014.

Banca Examinadora:

_____

Prof. Alexandre Moreira
IFSC

_____

Profª. Claudinice Carla Bertotti
IFSC

_____

Prof. Jorge Henrique Busatto Casagrande
IFSC

_____

Prof. Ederson Torresini
IFSC

DEDICATÓRIA

À minha mãe Edilha Vieira de Araújo, quem me ensinou a lição do silêncio a "ignorância" humana, e resistir à adversidade e travar brava luta de viver e vencer as etapas da vida, e ao meu Pai, Flávio de Araújo (*in memorian*), com amor eterno.

AGRADECIMENTOS

Agradeço a DEUS, por ter me dado saúde e força para superar as dificuldades, por ter me concedido o dom da perseverança, que me tem permitido buscar a realização dos meus sonhos.

Agradeço especialmente a minha mãe, Edilha, heroína, que me deu todo apoio necessário, amor incondicional e incentivo nas horas mais difíceis de desânimo e cansaço.

Agradeço ao meu marido, Marcelo, por ter suportado meu humor e pelo incentivo para eu continuar meus estudos.

Agradeço à minha linda filha, Flávia, por compreender a minha ausência e pela inspiração diária. Menina mais amada do mundo.

Às minhas sobrinhas; Amália, Amábile, Manoella e Mariana, e irmãs; Estela e Andrea e cunhados Sandro e Mário, que fizeram eu sorrir e acreditar no futuro próximo.

Às minhas primas, primos, tios e tias, a quem também amo muito, e tenho certeza que estão torcendo por mim. Em especial, Silvana e Rodrigo que estão sempre em contato.

A todos os meus amigos e amigas, em especial, à Vanessa, Elinara, Marilise, Marilene, Deise Will, Claudinice, Gerusa, Maria Aparecida, Fabiola, Alessandra, Wanderley, Mara, Sandra, e Maria Leda, que se tornou uma grande amiga, estes fizeram parte dos momentos mais difíceis desta jornada, dando-me força e coragem para eu não desistir, e a especial Prof. Ana Cristina Costa.

Agradeço ao meu Orientador, Prof. Alexandre Moreira e a minha co-orientadora Claudinice Bertotti pelo árduo trabalho de me orientar.

Agradeço aos meus colegas de turma, Ricardo Martins, e Helton Porto pela gentileza de emprestar os equipamentos e as aulas que me deram sobre o conteúdo do trabalho.

Agradeço a todos os professores e a toda equipe do IFSC SJ, em especial, a Maria Leda Costa Silveira, Prof. de Português Sueli, Prof. Diego, Prof.Vidomar, Prof. Fabio, Prof. Cláudia Castro, Prof. Ederson, Irene Martins, Sr. Nilton, Sra. Ada, Cida, Prof. André Alves e sua esposa Elizete Lanzoni Alves.

A todos que, direta ou indiretamente, fizeram parte da minha formação, o meu muito obrigada.

RESUMO

As Redes Privadas Virtuais têm sido uma excelente solução para interligar pontos geograficamente distantes, são estabelecidas por meio de uma estrutura de rede conectada à Internet, para isso é conveniente usar os Programas de Governo, pois minimiza custo, oferecendo às Escolas Públicas de Educação Básica, uma ligação entre elas.

Dessa forma, benefícios e informações poderiam ser trocados, bem como a padronização junto à ANATEL.

Mediante a combinação da estrutura existente nas escolas públicas atendidas por um *Internet Solution Provider* (ISP), ao conjunto de tecnologias que permitem uma rede privada virtual interligar pontos geograficamente distribuídos, foi que se extraiu o estudo que compete atender as Escolas Estaduais de Educação Básica, interligando por meio de uma rede *Virtual Private Network* (VPN), favorecendo as escolas conectadas por Satélite ou ADSL, tornando uma rede corporativa, podendo oferecer suporte técnico, acesso compartilhado de recursos computacionais de segurança, conteúdo, entre outros.

Palavras-chave: Redes Privadas Virtuais. Internet. ANATEL.

LISTA DE ABREVIATURAS

AAA *Authentication, Authorization, Accounting*

ADSL *Asymmetric Digital Subscriber Line*

ANATEL Agência Nacional de Telecomunicações

ATM Asynchronous Transfer Mode

ATU-C *ADSL Termination Unit Central Office*

ATU-R ADSL *Termination Unit Remote*

BRAS *Broadband Remote Access Server*

CE *Customer Edge*

CPE *Customer Premises Equipment*

DSLAM *Digital Subscriber Line Access Multiplexer*

FEC *Foward Equivalence Class*

FNDE Fundo Nacional de Desenvolvimento Educacional

GESAC Governo Eletrônico - Serviço de Atendimento ao Cidadão

GRE *Generic Routing Encapsulation*

IDH Índice de Desenvolvimento Humano

IEEE Instituto de Engenheiros Eletricistas e Eletrônicos

ISO *Organization for Standardization*

ISP *InternetSolution Provider*

KA *Above K*

K U *Under K*

LAN *Local Área Network*

LER *Label Edge Router*

LDB Lei de Diretrizes e Bases da Educação Nacional

LSP *Label Switch Path*

MEC Ministério da Educação

MPLS *Multiprotocol Label Switching*

NAS *Network Access Server*

NTE Núcleo Nacional de Tecnologia Educacional

ONU Organização das Nações Unidas

OSI *Open System Interconection*

P *Provider*

PBLE Projeto Banda Larga nas Escolas

PE *Provider Edge*

PPP *Point to Point Protocol*

PROINFO Programa Nacional de Tecnologia Educacional

PVC *Permanent Virtual Circuit*

TIC Tecnologia de Informática e Comunicação

VC *Virtual Circuit*

VCI *Virtual Channel Identifier*

VP *Virtual Path*

VPN *Virtual Private Network*

VPI *Virtual Path Identifier*

VRF *Virtual Routing and Forwarding*

VSAT *Very Small Aperture Terminals*

WAN *Wide Area Networ*k

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

1.1 MOTIVAÇÃO

O Governo Federal tem investido em Programas de uso de tecnologia de Informática nas escolas. Nesse sentido, os Estados, o Distrito Federal e os Municípios devem gerir e organizar seus respectivos sistemas de ensino como determina a Lei das Diretrizes e Bases da Educação Nacional (LDB).

O Governo Federal é responsável pelo investimento, mediante os Programas. Não é o Município, nem o Estado que investe, cada qual tem sua esfera, e é financiado pelo governo.

Estas escolas são autônomas entre si, ou seja, são independentes umas das outras, e os recursos tecnológicos oferecidos pelos Programas de governo são usados de forma isolada, sem compartilhamento de informação e de recursos entre elas. Além disso, não existe tecnologia que possa melhorar a prática pedagógica. Desta forma, tomando como base os ambientes tecnológicos oferecidos pelos projetos de governo, o Programa Nacional de Tecnologia Educacional (PROINFO) fornece os laboratórios equipados, e o Programa Banda Larga nas Escolas PBLE, que dá acesso à Internet por meio cabeado, e o Programa Governo Eletrônico - Serviço de Atendimento ao Cidadão *(*GESAC)[1] que atende às escolas nas quais não é possível o acesso Asymmetric Digital Subscriber Line (ADSL). Por isso, a proposta é criar a possibilidade de padronização, assim, formar uma rede corporativa entre as escolas conectadas, oferecendo um aprimoramento para o uso das tecnologias para estes programas governamentais.

O PROINFO é uma ação do Governo Federal em parceria com os Municípios, Estados e o Distrito Federal para promover o uso pedagógico de Tecnologia de Informática e Comunicação (TIC) 2 na rede pública de educação básica. Esse Programa é geralmente implantado nas escolas públicas, em salas com estruturas exigidas para formar ambientes tecnológicos (laboratórios), são equipados com auxílio do Programa, com computadores e recursos digitais. Os Laboratórios de Informática são montados pelo Ministério da Educação (MEC) e os governos locais (municipais e estaduais) prepararam a estrutura adequada para

---

[1] **GESAC** é um programa de inclusão digita do Governo Federal, coordenado pelo MEC voltado a promover inclusão digital e social em todo território nacional. (CARTILHA, 2007. p.5)
< http://www.institutoembratel.org.br/projetos/projetoGesac/swf/documentos/guias/CARTILHA_GESAC_02.pdf>

[2] **TIC** é um conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de *hardware*, *software* e telecomunicações, a automação e comunicação dos processos de negócios, da pesquisa científica e de ensino e aprendizagem.
< http://www12.senado.leg.br/manualdecomunicacao/glossario/tics>

receber esses laboratórios.

Outro Programa do Governo Federal que incentiva o uso de Informática nas escolas públicas urbanas é o Projeto Banda Larga nas Escolas (PBLE), que disponibiliza a conexão à Internet, de forma gratuita até 31 de dezembro de 2025, cabendo à Agência Nacional de Telecomunicações ANATEL[3] fiscalizar a velocidade de acesso.

Além dos Programas mencionados acima, o Programa GESAC (Governo Eletrônico de Serviço de Atendimento ao Cidadão), é oferecido para regiões rurais, nas quais as redes de telecomunicações tradicionais não oferecem acesso local à Internet em banda larga, utilizando-se da parceria entre a Secretaria Municipal de Educação, o FNDE e o Ministério das Comunicações, infocentros e escolas municipais que apresentarem baixo Índice de Desenvolvimento Humano IDH[4]. Dessa forma, podem utilizar-se do acesso à Internet via Satélite.

O projeto GESAC tem como meta conectar Laboratórios de Informática selecionados pelos governos estaduais, aos órgãos da administração federal e outras entidades da sociedade.

Foi neste contexto, de programas de inclusão digital, oferecidos pelo governo, que se pensou, em termos de aperfeiçoamento do uso dos recursos de telecomunicações, em uma Rede Privada Virtual (VPN) para propor uma forma de interligar os laboratórios da rede da escola.

A intenção é utilizar a infraestrutura pública existente (Internet) para trafegar dados através de um túnel lógico entre pontos autorizados da rede, interligando as escolas geograficamente distantes, de modo que a rede possa ser usada para compartilhar informação e recursos entre as escolas públicas de educação básica.

1.2 ORGANIZAÇÃO DO TEXTO

O texto compreende os objetivos a serem alcançados com o trabalho, tendo no capítulo 1, a introdução, motivação, organização do texto, os objetivos e a justificativa para o empreendimento deste estudo, momentos em que se busca conhecer melhor os Programas

---

[3] **ANATEL** Autarquia especial, criada pela Lei Geral de Telecomunicações (LGT), Lei 9.472, de 16 de julho de 1997, administrativamente independe, financeiramente autônoma e sem subordinação hierárquica a nenhum órgão de governo. Portal da Anatel. 2014.
< http://www.anatel.gov.br/Portal/exibirPortalInternet.do>

[4] **IDH** Índice de Desenvolvimento Humano, uma medida importante concebida pela ONU (Organização das Nações Unidas) para avaliar a qualidade de vida e o desenvolvimento econômico de uma população. (SIGNIFICADOS, 2014).
< http://www.significados.com.br/idh/>

Governamentais, os recursos computacionais oferecidos e as técnicas atuais de acesso de última milha de que dispõem as escolas atendidas pelos Projetos, para se tomar conhecimento dos problemas enfrentados e buscar uma forma de pontuar o uso de técnicas de rede, como maneiras mais simplificadas e dedicadas para o uso das tecnologias de informação e acesso à Internet.

No capítulo 2, será apresentada a fundamentação teórica, que descreve os principais conceitos para o desenvolvimento e conhecimento da tecnologia associada ao que se propõe.

O capítulo 3 descreve o cenário existente, como se encontra a rede da escola com a conexão à Internet, mediante a operadora de serviços ISP.

No capítulo 4 é demonstrado como seria montada e configurada a rede proposta, comparando-a com a estrutura atual, concluindo-se com a análise dos resultados. Uma vez definido o acesso à rede mundial de computadores, busca-se entender pontos pertinentes de uma VPN, para então, propor a forma de implementação de uma rede entre as escolas, como possível alternativa para minimizar as dificuldades técnicas encontradas, indicando-a também, como fonte de revisão do Programa Banda Larga nas Escolas (PBLE).

Nos capítulos 5, e 6, acontece a conclusão do trabalho e sugestão para trabalhos futuros, utilizando simuladores.

Ainda, no capítulo 7, constam os apêndices, nos quais são descritas as configurações que devem ser aplicadas em cada roteador simulado.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Por meio do estudo de técnicas de acesso de redes virtuais privadas, propor uma forma de padronização de interligação dos Laboratórios da rede da escola, com o auxílio de recursos do Programa Banda Larga nas Escolas, para suporte técnico remoto e possibilidade do uso de compartilhamento de recursos de segurança e conteúdo.

1.3.2 Objetivos Específicos

a) Estudar a aplicação prática de técnicas de acesso VPN, definindo como configurar os equipamentos da estrutura proposta para o seu funcionamento, por meio de uma rede de compartilhamento de recursos geograficamente distribuídos;

b) Apontar o uso das técnicas de acesso VPN como revisão das especificações da ANATEL para o PBLE;
c) Consolidar o aprendizado de redes de computadores adquirido durante o curso de Sistemas em Telecomunicações, pelo estudo da formação da rede VPN.

1.4 JUSTIFICATIVA

Este trabalho visa a um estudo das técnicas de acesso VPN com o intuito de definir uma estrutura de redes que permita a interligação de pontos geograficamente distribuídos. As escolas recebem os recursos dos programas governamentais; porém, trabalham de forma isolada, permitindo-lhes que seja possível receber suporte técnico remoto para a operação e a manutenção da rede, bem como, o acesso compartilhado a recursos computacionais de segurança, conteúdo, entre outros.

Mediante o estudo das técnicas de acesso, será explicada a forma de configurar os equipamentos envolvidos na construção da VPN, bem como, criar o túnel, tanto para ADSL, quanto Satélite.

Com a VPN, será estabelecido um túnel sobre a rede física, criando uma interligação lógica de pontos geograficamente distribuídos, pré-determinados, na perspectiva de possibilitar uma resposta positiva, pelo uso das VPNs agregadas aos Programas de governo.

Neste sentido, a relevância deste estudo, é que seu resultado poderá ser apresentado para ANATEL como possibilidade de uso das mesmas quando da nova revisão das especificações dos laboratórios informatizados da rede das escolas.

2 FUNDAMENTAÇÃO TEÓRICAS

Neste capítulo são apresentados os conceitos e ferramentas utilizadas para o estudo das técnicas de acesso VPN a fim de que haja melhor, compreensão deste trabalho.

2.1 CONCEITO DE VPN

As redes privadas virtuais, cuja sigla VPN vem do inglês, *Virtual Private Network*, são redes que usam como base a Internet; porém, mantendo as características de segurança e privacidade na interligação de pontos geograficamente distantes. É considerada uma rede, pois interliga os equipamentos de comunicação de dados; e é privada, porque é controlada pelo próprio usuário, tendo por base uma estrutura de *Internet Solution Provider* (ISP), *o*u provedores dos serviços de Internet, no caso do Brasil, principalmente operadoras de telecomunicações ou televisão por assinatura, além de umas poucas empresas independentes, cuja outorga é liberada pela Anatel.

Apesar de a rede se estruturar por intermédio da Internet, é diferente, pois é privada, o que quer dizer que não é aberta a todo o público que navega na Rede Mundial de Computadores.

E, por fim, é virtual, já que não tem enlaces dedicados entre seus extremos; no entanto, isso é transparente para o usuário, que não percebe tratar-se de enlaces virtuais, uma vez que têm as mesmas características de enlaces ponto-a-ponto.

Segundo Valente (2001), uma VPN interliga sites de uma mesma rede que se deseja comunicar, e pode ser considerada como objeto de conectividade.

Tais afirmações explicam que VPN’s interligam, por meio de uma rede compartilhada, um conjunto restrito de pontos, e é importante salientar, porém, que os pontos conectados por uma VPN têm a conectividade regida por políticas administrativas.

Segundo Oliveira (2012), normalmente são criadas redes privadas em empresas com muitas filiais para uma comunicação restrita aos pontos remotos e sua matriz.

Dessa forma, significa que uma VPN é uma solução simples e flexível e acabou por se tornar uma ferramenta de tunelamento para os provedores de serviços de Internet, uma vez que os ISPs poderiam usar a mesma infraestrutura existente, emulando enlaces ponto-a-ponto entre os endereços do cliente, para atender os moldes de interligação, mesmo em áreas geograficamente distribuídas.

A VPN oferece ganhos, uma vez que pode compartilhar meios físicos (nos pontos de

concentração), não exigindo, para cada conexão, meios ponto-a-ponto. O acesso só é estabelecido a qualquer lugar onde haja conexão com a Internet, tornando-se uma solução amplamente difundida. Esta rede é facilmente escalável, pois a medida que houver a necessidade, serão inseridos novos pontos de presença.

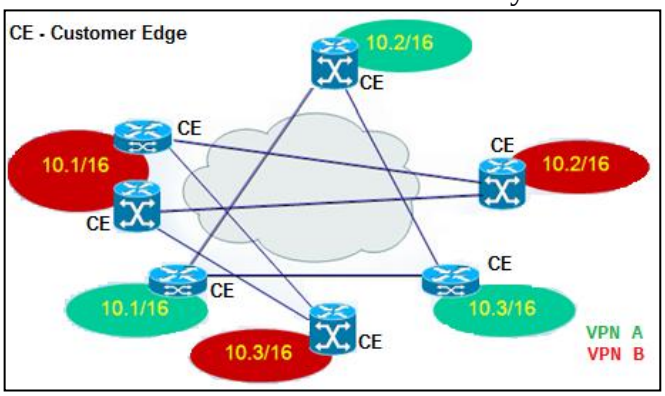
A propósito, a VPN, baseia-se na tecnologia de tunelamento, onde os túneis, são o caminho lógico percorrido pelos pacotes ao longo da rede, ou seja, o tunelamento é o processo de encapsular um protocolo dentro de outro, podendo, antes de encapsular, criptografar o pacote para que não seja inteligível sem a chave de encriptação. Após alcançar o destino, o pacote é desencapsulado e encaminhado ao ponto final de interesse.

Os modelos de tunelamento para VPN são de dois tipos, quais sejam: *Overlay* e *Peer-to-peer*.

No modelo *overlay*, os equipamentos do cliente são responsáveis por toda lógica de funcionamento, ou seja, o cliente é responsável pelo desenho e pela operação da estrutura VPN e a operadora de telecomunicações fornece os enlaces físicos ou circuitos que permitam acesso a equipamentos de rede *Frame-relay*[5] ou ATM. Isso implica que o cliente detenha conhecimentos de roteamento IP e mapeamento. Na construção das redes *overlay*, são aplicados túneis GRE (Generic Routing Encapsulation), L2TP ou IPSec.

A seguir, segue a figura representando o modelo *Overlay*:

FIGURA 1 - Modelo Overlay



Fonte: Valente, 2001, p.22.

Neste tipo de processo, o provedor de serviços não conhece as rotas do cliente, não troca informações de roteamento, apenas atende o cliente com circuitos virtuais privados (PVC's).

---

5 Frame Relay: Tecnologia de transmissão de dados.
TANENBAUM, Andrew. S. Redes de Computadores. Rio de Janeiro. Ed. Elsevier, 2003. p. 64

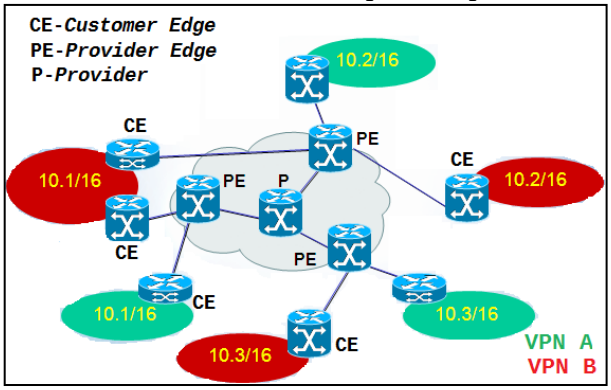
Segundo Oliveira (2012), entre o roteador do cliente e o provedor de serviços, neste modelo, não acontece nenhum processo. O provedor de serviço não visualiza as rotas do cliente.

A necessidade da conectividade completa entre todos os pontos, é um problema para o modelo *overlay*, ou seja, cada conexão, de cada ponto, necessita de uma conexão e um roteamento ponto-a-ponto com todos os outros pontos da VPN.

E, no modelo, *peer–to-peer*, o operador de serviços de telecomunicações atua na estrutura funcional da VPN, onde os PEs (*providers edges*), roteador de borda da operadora, e os CEs (*customer Edges*) roteador de borda do cliente, formam pares na definição do processo de roteamento.

A seguir, a figura representando o modelo *peer-to-peer:*

FIGURA 2 - Modelo *peer-to-peer*



Fonte: Valente, 2001, p.29.

> O modelo par-a-par não requer a criação de circuitos virtuais e também garante privacidade e isolamento entre os diferentes clientes através de configurações de filtros de pacotes, tais como as listas de acesso (access list), controlando assim, os dados para os clientes e os dados originados destes. Outra maneira de proporcionar o isolamento e a privacidade entre os clientes é através de filtros de rotas, anunciando ou parando rotas para determinados clientes. Os dois métodos podem também trabalhar em conjunto (De Ghein apud Oliveira, 2012, p.51).

Neste sentido, o cliente pode ter pouco ou nenhum conhecimento de roteamento, além do que, há enorme flexibilidade em termos de conexões e pontos de presença, que podem ser agregados à rede há qualquer tempo.

2.2 ADSL

Devido à excelente cobertura e capilaridade das redes telefônicas, nasceu a família DSL (Digital Subscribers Line ou Linha digital de assinante).

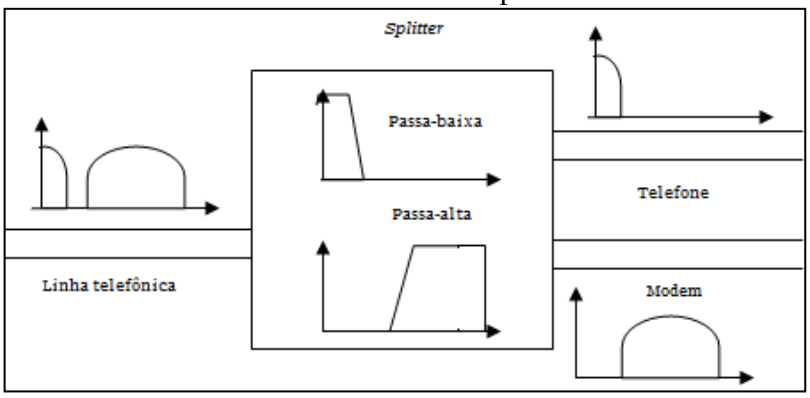
O termo ADSL ou Asymmetric Digital Subscriber Line sucede do tipo de utilização do tráfego ser assimétrico, ou seja, utiliza-se mais a conexão para receber informação do que para o envio, e como esta transmissão acontece sobre a mesma rede de acesso da linha telefônica comum, há um excelente alcance, atingindo assim, os usuários domésticos, o que popularizou seu uso.

A linha telefônica comum, no entanto, é subutilizada, pois a voz ocupa apenas uma banda de 4 kHz, e é comum se obter até 2 MHz de banda em um par metálico, ou seja, agregando-se ao par trançado às técnicas de ADSL, ele se converte em meio para três canais distintos: de voz, transmissão e recepção de dados.

Para tanto, o dispositivo comumente conhecido como *modem*, (contração dos termos modulador e demodulador) que modula um sinal digital na onda portadora analógica, que se transmite pela linha telefônica, e que demodula o sinal analógico e reconverte-o para o formato digital ao chegar ao destino, o ATU-R (ADSL Termination Unit Remote), na residência do usuário, é responsável por permitir o uso do cabeamento para a transmissão de dados, com modulação acima da frequência de voz.

Para separar dados e voz, são instalados no lado da central de operação e no cliente, separadores, os chamados *splitters*, que são filtros passa-baixa e passa-alta, agindo como separadores de dados e voz, como mostrado na figura abaixo.

FIGURA 3 - Filtro splitter



Fonte: Monteiro, 2007, p.20.

Após a separação das faixas de frequência respectivas, com as informações de voz, que seguem para o caminho usual de comutação, as aplicações de multimídia e transferência de dados são encaminhadas para o DSLAM (*Digital Subscriber Line Access Multiplexer* ou Multiplexador de Linhas de Acesso de Assinante).

O DSLAM é um dispositivo que interliga as várias DSLs a uma linha “tronco”,

conduzindo-as ao *backbone*[6]. É, na verdade, o suporte de *hardware* a uma coleção de *modems*, na qual cada *modem* das placas que o compõe (porta) comunica-se com um único *modem* DSL. O DSLAM dispõe de comutador de dados (switch) e um multiplexador. Utilizando-se de técnicas de multiplexagem, agrega o tráfego de voz e dados em um sinal composto (HENZ, 2008, p.22).

No envio do sinal para o cliente (*download*), multiplexa a voz e o tráfego de dados sobre a linha DSL do cliente.

Quando recebe do cliente a informação (*upload*), separa as chamadas telefônicas de saída dos sinais de dados e direciona os dados para a rede de transporte adequada, e os sinais telefônicos para o comutador de voz.

Segundo Henz (2008. p.20), para melhor explicar o funcionamento, na mesma linha telefônica é transmitida simultaneamente o sinal de dados e voz, entrando no filtro *splitter*, no qual é separado a voz dos dados. A voz encaminhada para a rede de comutação de circuitos da companhia telefônica, e os dados são encaminhados para o DSLAM, que internamente tem um *modem* ADSL, que é identificado por um endereço chamado porta, cada porta corresponde a um assinante.

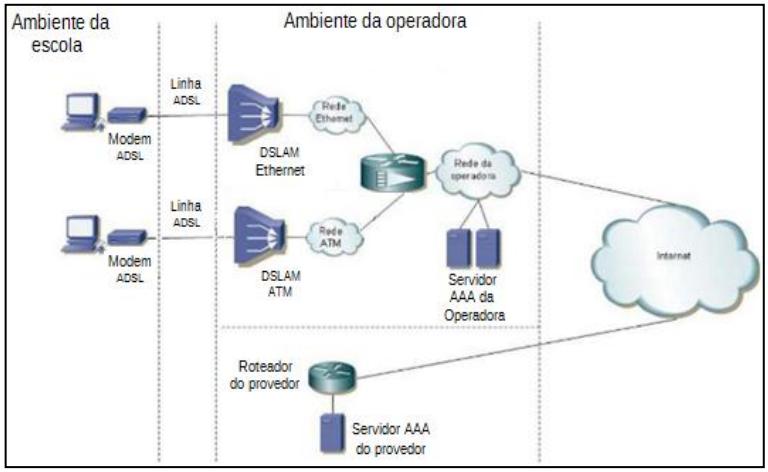
Entende-se que o uso da rede telefônica para o tráfego de dados por meio do uso das técnicas ADSL, aproveita de todos os elementos que compõem aquela estrutura, aprimorando-a.

Segue a figura mostrando elementos que compõem a rede ADSL:

---

[6] *Backbone* é o trecho de maior capacidade da Internet e tem o objetivo de conectar vários pontos da Rede. Em português, significa espinha dorsal. É o termo utilizado para identificar a rede principal pela qual os dados de todos os clientes da Internet passam.
< http://www.tecmundo.com.br/conexao/1713-o-que-e-backbone-.htm>

FIGURA 4 - Estrutura do acesso ADSL

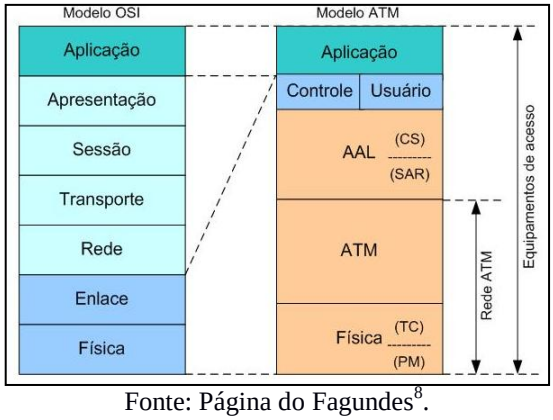


Fonte: Henz, 2008, p.38

As informações encapsuladas no DSLAM, seguem via um tronco de agregação, baseado em links de fibras ópticas, para os switches ATM ou Ethernet. A tecnologia ATM Asynchronous Transfer Mode, traduzida para o português como Modo de Transferência Assíncrono, é uma arquitetura de rede que opera na camada de enlace nível 2 do modelo OSI[7], e que transmite todas as informações através das células, totalizando 53 bytes entre cabeçalho e carga útil.

Segundo Fagundes, ele mostra o modelo OSI em função do Modelo ATM, onde todas as camadas deste modelo têm suas funcionalidades, conforme se pode observar abaixo a figura que ilustra o modelo ATM:

FIGURA 5 - Modelo ATM



Fonte: Página do Fagundes[8].

[7] **OSI**, Modelo OSI é um modelo de referência da ISO Organization for Standardization, composto por 7 camadas, em que cada camada realizada funções específicas.
TANENBAUM, Andrew. S. Redes de Computadores. Rio de Janeiro. Ed. Elsevier, 2003. p. 40
[8] Disponível em: www.fagundes.com Acesso em: 19/08/2014

Na camada FÍSICA é mapeada as células ATM no formato dos frames das redes de transmissão, e são temporizados os bits do frame, de acordo com o relógio de transmissão.

Na camada ATM é processada os diferentes tipos e classes de serviço, além disso, controla o tráfego da rede. Esta camada trata todo o tráfego, nos equipamentos de origem e destino, minimizando o processamento da rede e aumentando a eficiência do protocolo, a dependência de todas as camadas superiores.

Na camada AAL, a informação do usuário é convertida e preparada para o ATM, de acordo com o tipo de serviço, além de controlar as conexões virtuais, converter e preparar, fragmenta a informação para ser encapsulada na célula ATM, usada tanto para redes locais LANs, como para redes geograficamente distribuídas, WANs, que suporta vídeo, dados e voz em tempo real.

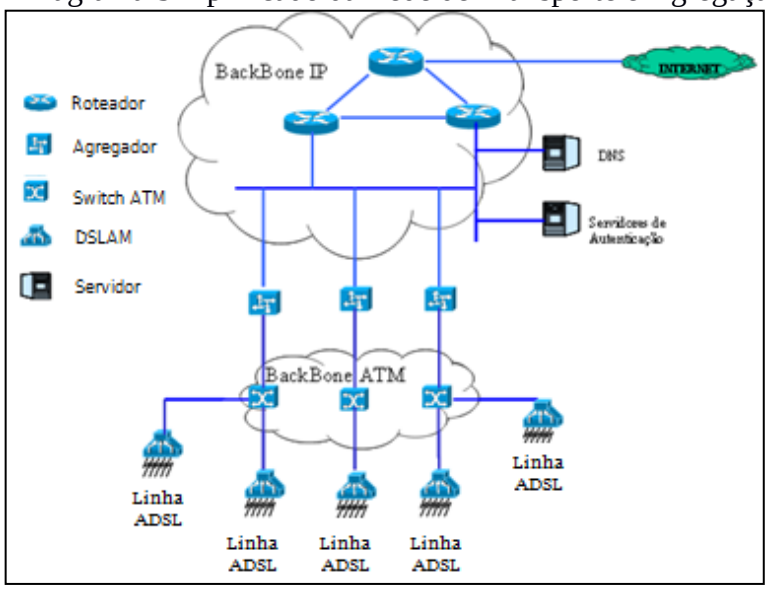
O ATM atende as redes locais geograficamente distantes que suportam a comunicação de voz, vídeo e dados.

Segundo Nunes (2007, p. 18), *Ethernet* é a arquitetura utilizada em redes locais de computadores (LAN), padronizada pelo Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE), que define, para a camada física, quais tipos de cabos podem ser utilizados e como os sinais são transmitidos.

Quando se trata de *switches Ethernet*, o reconhecimento das conexões *Ethernet*, é por *VLANs* (*Virtual Local Area Network*), e em *switches* ATM, é por PVCs (*Permanent Virtual Circuit*). Os *switches* são responsáveis por concentrarem as terminações dos DSLAMs.

Para terminar as conexões iniciadas em cada *modem*, de forma que possam seguir para a camada de rede, através da obtenção de um endereço IP e então navegar na Internet, dos *switches*, as informações seguem aos agregadores, em topologias similares. E os a que mostra a figura abaixo:

FIGURA 6 - Diagrama Simplificado da Rede de Transporte e Agregação do ADSL.



Fonte: Henz, 2008. p. 23

Os agregadores, terminadores ou *BRAS* (*Broadband Remote Access Server*) ou ainda *NAS* (*Network Acess Server*), são termos usados para este equipamento, este, por sua vez, estabelece a conexão lógica entre o *modem* com a rede da operadora.

Segundo Gruszynski (2008, p.37), no documenento do equipamento, diz que um lado é voltado ao assinante, e outro lado, voltado à rede; onde, o lado do assinante refere-se às interfaces utilizadas para conectar o BRAS às redes ATM ou *Ethernet*, onde se encontram os DSLAMs e, outro lado da rede, conecta com os demais elementos que compõem a rede de comunicação de dados do ISP.

Significa que, as configurações de perfil designadas aos usuários do serviço ADSL para cada *VLAN Ethernet* ou Circuitos Virtuais (VC) ATM, são declaradas no agregador, bem como as condições de serviço, além da conexão de usuário, no tangente à obtenção de serviços designados por AAA (*authentication, Authorization, Accounting*), em português significa Autenticação, Autorização e Contabilidade, estão estabelecidos de forma que permitam a decisão de aceitar ou declinar a solicitação de navegação daquela conexão ADSL. No caso de consentir a conexão, o modem que fez a solicitação, recebe um IP, e já pode, através dos roteadores do ISP, entrar na Internet.

Lembrando que as escolas de educação básica recebem a conexão à Internet, utilizando a tecnologia ADSL ou Satélite. Quanto a este tópico, far-se-á a seguir, um breve conceito.

2.3 SATÉLITE

Um satélite de comunicação pode ser considerado um grande repetidor de micro-ondas no céu. O satélite contém diversos *transponders*. O modo de operação funciona como espelho *bent pipe*[9], no qual os feixes descendentes podem ser largos, cobrindo uma fração substancial da superfície terrestre; ou estreitos, cobrindo áreas com apenas centenas de quilômetros de diâmetro.

A propósito, o *transponder* de um satélite de comunicações é um conjunto de unidades interligadas que formam um canal de comunicação entre o receptor e as antenas de transmissão.

Cada *transponder* pode usar várias frequências e polarizações, com a finalidade de aumentar a largura de banda disponível. (TANENBAUM, 2003, p.116).

Segundo Abramson (apud Tanenbaum, 2003, p.119), inúmeras aplicações comerciais, emissoras de televisão, governos e instituições militares, disputam pelos *slots* de órbita. A criação de microestações chamadas VSATs[10] - *Very Small Aperture Terminals* impulsionaram o uso dos satélites para transmissão de dados em banda larga.

Os pequenos terminais VSAT têm antenas de 1 metro ou menos (O tamanho da antena VSAT é limitado em aproximadamente 2.4m), e podem emitir cerca de 1watt de energia. Geralmente, o *uplink* é adequado para 19,2Kbps, mas o *downlink* com frequência exige 512 kbps ou mais. Em muitos sistemas VSAT, as micros estações não têm energia suficiente para se comunicarem diretamente com as outras. Para isso, é necessária uma estação terrestre espacial, o *hub*, com uma grande antena de alto ganho para retransmitir o tráfego entre VSATs ou concentrar o tráfego que provém de vários hóspedes, e gerar, de novo, o sinal.

Para o projeto GESAC, são usadas combinações de interligação terrestres e satélites, onde um trecho (última milha) é feito por satélite, no caso *VSATs* e, via estações HUB, e estas, através das operadoras de telecomunicações, interligam-se aos grandes centros de forma que a Internet seja alcançada.

Segundo Nascimento (2012), há 44 satélites de telecomunicações que operam banda

---

[9] ***bent pipe*** é quando um sinal de chamada ou bit de dados é enviado a partir do ponto de origem, para um satélite e, em seguida, volta para a Terra, dirigido a outro destino, muitas vezes localizados longe.
TANENBAUM, Andrew. S. Redes de Computadores. Rio de Janeiro. Ed. Elsevier, 2003. p.116

[10] **VSATs** são pequenas estações de satélite terrenas transportáveis e normalmente conectadas a uma rede, composta pelas estações terrenas transportáveis e pelas estações concentradoras.
TANENBAUM, Andrew. S. Redes de Computadores. Rio de Janeiro. Ed. Elsevier, 2003 p.119

larga em banda Ku[11] (2,5Gbps), utilizada pelas VSATs; no entanto, o alto custo que foi empregado para a manutenção deste sistema, tende a deixá-lo economicamente inviável. Uma nova e mais barata alternativa de grande potencial tecnológico, a banda Ka[12](100 Gbps) já se encontra em funcionamento, e comercialização no Brasil desde setembro de 2014, depois da ANATEL ter licitado o direito de exploração de satélite de quatro posições orbitais, cujos segmentos espaciais devem cobrir 100% do território nacional, para atender, tanto banda Ku, principalmente para o DTH[13], quanto Ka.

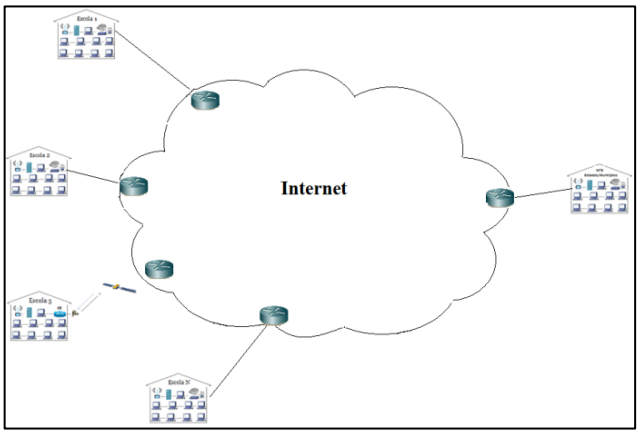
[11] **Ku,** é a faixa de frequência, onde utiliza um sinal de frequência de 14 GHz no sentido Terra/Satélite e 12GHz no sentido Satélite/Terra, com espectro (IEEE) de 13.35 até 17.25.
[12] **Ka**, é empregada para o termo K-*above band*, utilizada na comunicação por Satélite, sendo a parte do espectro eletromagnético, na faixa de micro-ondas compreendida entre as frequências de 27 e 40 GHz.
[13] **DTH** é a modalidade de transmissão de televisão digital via satélite. Disponível em:< http://www.futurecom.com.br/blog/o-que-e-dth/ >

3 CENÁRIOS

3.1 CENÁRIO ATUAL

Neste cenário está sendo mostrada a figura que simboliza a estrutura da rede das escolas públicas, todas têm seus laboratórios informatizados, e são ligadas individualmente à Internet por meio de um ISP.

FIGURA 7 - Cenário atual da rede das escolas.



Fonte: Elaborada pela autora, 2014.

A figura acima representa às escolas ligadas à internet via *ADSL* ou Satélite, desta forma, conectadas pelos programas de governo PBLE ou GESAC, em laboratórios da rede da escola.

3.1.1 Cenário Atual ADSL

De acordo com o que já foi abordado na fundamentação teórica (2), ter-se-á, agora o entendimento de como o ADSL e o Satélite são utilizados para o alcance da Internet na rede da escola.

Cada escola recebe um *modem* ligado a uma linha telefônica comum. Sendo assim, chamaremos este *modem*, de *CPE* (*Customer Premises Equipment*)[14] ou *ATU-R* (*ADSL Termination Unit Remote*) .

O CPE permite a abertura e encerramento das sessões *PPP Point to Point Protocol*,

[14] CPE *Customer Premises Equipment*, é um nome genérico, dado aos equipamentos de rede que estão localizados na ponta do acesso do usuário/assinante de um serviço de telecomunicações.
< http://www.cedet.com.br/index.php?/O-que-e/Telecom/cpe-customer-premises-equipment.html>

que é um protocolo que suporta ou encapsula vários protocolos da camada de rede, para o transporte, por meio do laço *ADSL* até o *DSLAM*.

O *PPP* pode operar através de uma rede ATM ou uma rede *Ethernet*, e tal escolha é feita no momento da configuração do *modem* e ou a instalação, do acesso pela operadora, que é quem vai determinar qual rede atenderá aquele acesso.

O DSLAM, conhecido como *ATU-C* (*ADSL Termination Unit Central Office*), recebe os acessos do lado da central telefônica, e interliga as várias *DSLs* (*Digital Subscriber Lines*) a uma linha "tronco", conduzindo-as ao *backbone. O DSLAM,* quando recebe do cliente a informação (*upload*), separa as chamadas telefônicas de saída dos sinais de dados e direciona os dados para a rede de transporte adequada, e os sinais telefônicos para o comutador de voz.

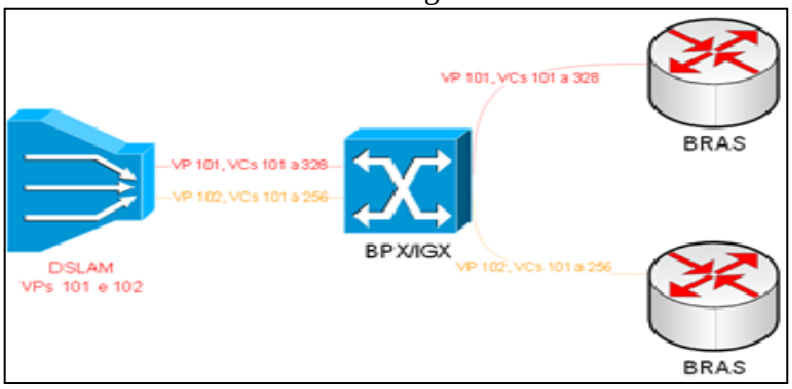
Ou seja, quando a escola liga o *modem*, que já está conectado a uma linha telefônica comum existente, dotada de um filtro de linha, que é um componente que se encontra conectado à tomada telefônica e elimina eventuais ruídos do *modem* na linha, um usuário e senha previamente gravados no *modem*, são encapsulados no sinal repassado pelo *modem*, que seguem via os cabos da linha, até a estação telefônica. O sinal atinge o DSLAM, onde o splitter filtra o sinal de voz, quando existente, encaminhando-o a comutação e, o sinal de dados é agrupado ao sinal das demais portas para, via um tronco de agregação (*uplink*) chegarem aos *switches* ATM ou *Ethernet*, e destes, aos agregadores e roteadores do *backbone* da operadora.

A comutação em *switches ATM* se processa por VP *Switching* (comutação de *Virtual Path*) e, portanto, cada DSLAM, para ter sua terminação reconhecida é identificado por um *VPI* e para cada porta física do DSLAM um *VCI* é atribuído. VPI e VCI *Virtual Path Identifier* [15]e Virtual *Channel Identifier*, respectivamente, são campos do cabeçalho da célula ATM responsáveis por levar as mesmas de um ponto a outro.

A seguir, a figura ilustrando a configuração do *DSLAM ATM*, configurado com *VCI*, e terminado no *BRAS* destino.

[15] VPI *Virtual Path Identifier* e VCI *Virtual Channel Identifier* juntos servem para identificar a rota em que o modem ADSL vai usar na rede de telefonia até chegar ao roteador para o acesso a internet.

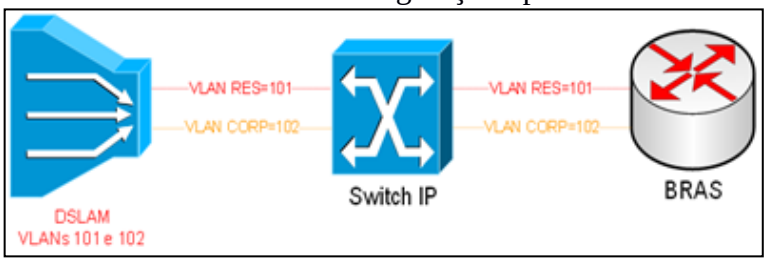
FIGURA 8 - DSLAM com dois VPNs configurados terminados em BRAS distintos.



Fonte: Henz, 2008. p.40.

Já, para os *switches Ethernet*, os *DSLAM* são identificados via *VLAN's* e, neste caso, a autenticação dentro de uma mesma VLAN só é possível por meio do mac address do *modem* conectado.

FIGURA 9 - DSLAM Ethernet com configuração típica – 2 VLANs configuradas.



Fonte: Henz, 2008. p. 41

Ou seja, as tabelas dos *switches ethernet* devem conter qual a interface de entrada do(s) *DSLAM*(s) e sua(s) respectiva(s) *VLAN*(s) e nos *switches ATM*, qual a interface de entrada de cada *DSLAM*, com o seu respectivo VP e sua gama de *VC*'s (*VC* inicial e VC final).

Quando o sinal da escola 1, chega ao DSLAM ATM, seu *PVC* originalmente configurado no *modem*, como por exemplo, VP 0 e VC 40 é alterado para o respectivo *VP* do *DSLAM* (por exemplo, 101) e *VC* da porta (por exemplo, 10) e através deste novo identificador, seguirá via *Switch ATM* até seu respectivo agregador.

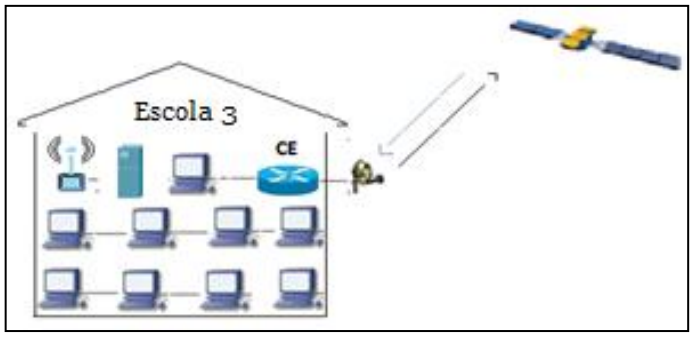
Do mesmo modo, quando o sinal da escola 2 chega ao DSLAM *ethernet*, seu *PVC* original, por exemplo, VP 0 e VC 40, será alterado para o respectivo número da VLAN, por exemplo 102, seguindo com tal identificação até o agregador.

Então, o agregador, terminador ou *BRAS* (*Broadband Remote Access Server*) ou ainda, *NAS* (*Networ Access Server*), é o equipamento que finaliza conexões *ADSL*, ou seja, é aqui que a sessão PPP é terminada, e um IP válido é fornecido para que o cliente possa navegar na Internet.

Muito embora os conteúdos possam estar em repositórios de dados dispersos em várias unidades e acessíveis via Internet, através de *ADSL*, seu compartilhamento não é intuitivo, como seria se houvesse um sistema interligado. Mesmo que haja um padrão inicial de equipamentos e instalação dos laboratórios, a manutenção dos ambientes acaba se perdendo por falta de uniformização e mão de obra capacitada, e também ferramentas de autenticação, monitoramento e segurança de acesso dificilmente são implementadas por serem de complexa administração pela mão de obra técnica disponível nas escolas.

3.1.2 Cenário Atual – Satélite

FIGURA 10 - Cenário atual, escolas beneficiadas via Satélite



Fonte: Elaborada pela autora, 2014.

Este cenário simboliza uma escola da grande Florianópolis que é atendida com conexões por meio de Satélite, através do programa GESAC. Este programa foi criado pela Portaria nº 256 de março de 2002, que permite a universalização do acesso às informações e serviços do governo eletrônico.

Para atuar nos pontos de presença[1] do GESAC, são elencados profissionais com "nível médio completo, sendo desejável nível superior, preferencialmente em Humanas. Além de experiência em projetos sociais, conhecimentos em Educação Popular, em articulação de redes solidárias e em formação de agentes sociais. Conhecimento das Tecnologias de Informática e Comunicações, preferencialmente aquelas desenvolvidas em ambientes livres.

Pontos de presença são pontos de acesso à Internet disponibilizados pelo GESAC com um número mínimo de cinco máquinas conectadas, e aberto ao público em geral. Quem tiver interesse em obter acesso à Internet, via conexão GESAC, além de atender às premissas de permitir acesso ao público em geral e ter ambiente adequado para a instalação dos equipamentos, deve estar sob uma Instituição responsável, a qual encaminha o pedido e assina o contrato com o Ministério das Comunicações. No caso de escolas, por exemplo, é o

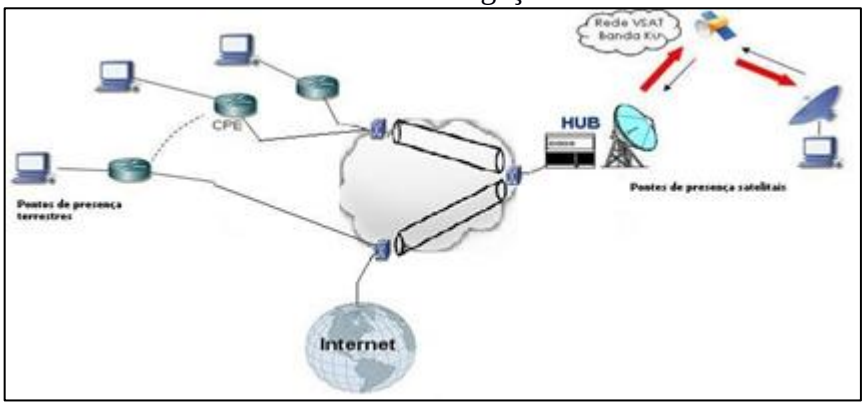
Ministério da Educação que se configura como a Instituição responsável pelo envio da proposta ao Ministério das Comunicações. (GESAC, 2010).

Segundo GESAC (2010), na região Sul do Brasil foi distribuído 904 pontos de presença, com o auxílio do Projeto, sendo que em Santa Catarina foram 143 pontos.

Foi por meio da visita em uma escola da Grande Florianópolis, foi percebido que a escola possui um ponto de presença, antena e circuito da Hughes/Oi.

Atualmente, duas empresas prestam serviço de telecomunicações para o GESAC, por meio de um Consórcio denominado Conecta Brasil Cidadão. As empresas selecionadas foram a Embratel, que presta serviços de conexão, via Satélite, e a Oi-Brasil Telecom, que presta serviços de conexão terrestre à rede GESAC (Medeiros, 2009, p. 31), e o atendimento já acontece mediante o uso de VPN.

FIGURA 11 - Estrutura de interligação do sistema GESAC.



Fonte: Elaborada pela autora, 2014.

A figura acima é uma representação de como os pontos de presença GESAC, para as redes das escolas, serão atendidos por Satélite. A estrutura GESAC, no entanto, prevê pontos de concentração terrestres, os quais fazem a etapa de segurança, de encaminhamento para os serviços de conteúdo e acesso à Internet.

Como foi descrito no item 3.1.1 Cenário atual – ADSL, os acessos terrestres têm seus *PVC*'s ou *VLAN*'s definidos, de tal forma que possam ser encaminhados, via o perfil designado no agregador para os túneis formados dentro da rede das operadoras que compõem o consórcio Conecta Brasil Cidadão. Eventualmente, tais pontos terrestres podem ser dotados de circuitos ponto-a-ponto ou mesmo *metro-ethernet*[16], para o acesso à rede das operadoras,

[16] *Metro-Ethernet*,é um modo de utilizar redes Ethernet em áreas Metropolitanas e geograficamente distribuídas. <http://blog.ccna.com.br/2008/04/27/metro-ethernet/>

conforme necessidade de disponibilidade de banda, já que podem ter que atender inúmeros acessos remotos.

A estação Hub, concentradora de acessos Satélites é quem fará a conexão com o serviço de agregação da operadora, encaminhamento ao túnel VPN.

A maneira como se processa a comunicação entre os pontos de presença remotos e os concentradores, encontra-se descrita na sequência deste trabalho, no Cenário Proposto, item 4.

3.2 VISITA À ESCOLA PÚBLICA DE EDUCAÇÃO BÁSICA

A visita foi realizada na Escola Básica Tenente Almáchio, localizada na Base Aérea de Florianópolis.

Vale salientar que, para a visita, foi obrigatória a emissão de uma autorização emitida pelo Núcleo de Tecnologia Educacional – NTE – da grande Florianópolis; documento esse, exigido pela Instituição visitada.

Dessa forma, foi possível conhecer a estrutura do laboratório implantado com os recursos do Governo Federal, já estudados no presente trabalho.

Normalmente, o laboratório é utilizado pela comunidade escolar para pesquisas de conteúdo e trabalhos escolares por disciplina, sempre acompanhados pelo respectivo professor, que também controla o tipo de acesso, além do monitor contratado para o laboratório da escola.

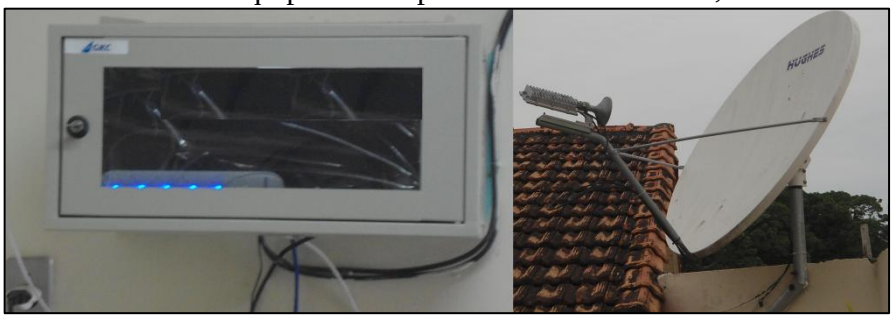
A figura, a seguir, mostra-nos o laboratório equipado com computadores, esta visita, trouxe uma visão de como os recursos estão instalados.

FIGURA 12 - Foto do laboratório da rede da escola.

Fonte: Elaborada pela autora, 2014.

A foto abaixo nos mostra a antena (antena HX50, 120 cm, Hughes) instalada na escola, conforme determina o programa GESAC, atendendo sua conexão com a Internet, via Satélite.

FIGURA 13 - Foto de equipamentos para acesso via Satélite, na rede da escola.



Fonte: Elaborada pela autora, 2014.

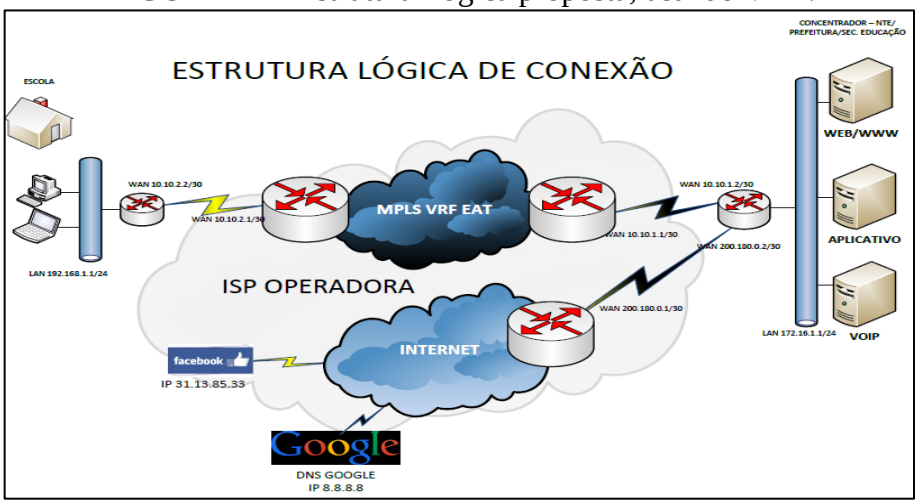
Esta é a estrutura existente atualmente nas escolas, as figuras ilustram os equipamentos da rede da escola, com acesso à Internet via o projeto GESAC.

Com a ideia de otimizar recursos e, principalmente, mão de obra com conhecimento tecnológico, foi pensado em uma técnica que favoreça a estrutura existente, conforme mencionado no embasamento teórico.

4 CENÁRIO PROPOSTO

Dando prosseguimento ao estudo, tem-se aqui a figura que ilustra a estrutura lógica da rede *VPN* a qual se objetiva estabelecer. Pode-se observar que o concentrador e a escola estão ligados ao *Backbone* ISP, dentro da estura da rede *MPLS* (estrutura existente e implantada na rede do ISP), foi criada uma VRF com nome eat (estudo de aplicações de técnicas de acesso), configurada, caracterizando o túnel MPLS, entre a rede da escola e o concentrador.

FIGURA 14 - Estrutura Lógica proposta, usando VPN.



Fonte: Elaborada pela autora, 2014.

Na sequência, será abordado como se pretende atender a estrutura, mostrando a simulação, usando equipamentos reais, equipamentos CISCO, que são utilizados pela estrutura ISP. Dessa forma, serão configurados nos equipamentos parâmetros para a criação da VPN, a fim de aplicar testes, simulando um cenário real para a comprovação do funcionamento da VPN proposta.

4.1 A PROPOSTA

Como visto no início do capítulo 3, cenário atual, sabe-se que as escolas são dotadas de acessos ADSL ou Satélite para comunicação com a Internet.

Muito embora os conteúdos possam estar em repositórios de dados dispersos em várias unidades de ensino e, acessíveis via Internet, para o usuário final ou mesmo equipes de implantação e manutenção, seu compartilhamento não é intuitivo, como seria se houvesse um sistema interligado. Mesmo que haja um padrão inicial de equipamentos e instalação dos

laboratórios, a manutenção dos ambientes acaba se perdendo por falta de uniformização e mão de obra capacitada. Nesse sentido, ferramentas de autenticação, monitoramento e segurança de acesso dificilmente são implementadas por serem de complexa administração pela mão de obra técnica disponível nas escolas.

O uso da VPN propõe minimizar tais efeitos, além de prover a interligação dos pontos geograficamente distribuídos, de forma a melhorar o fluxo de informações com flexibilidade e economia, do ponto de vista do uso de recursos já existentes e uma boa flexibilidade para ampliação e implementação de soluções (lançando-se mão de concentradores de conteúdo regionais, definindo apenas um concentrador que atenderá todas as escolas contempladas pelo NTE[17] regional, por exemplo).

O que se espera, basicamente, é dispor de recursos de redes locais, onde, para o usuário, pareça estar conectado à Internet, sem perceber que está utilizando uma VPN, mantendo-se assim, as mesmas funcionalidades de acesso e segurança, de uma rede privada, ampliadas em níveis regionais. Uma vez que a *VPN* estabelece sub-redes, sobre rede física geograficamente distribuída. Esta rede virtual fornece um serviço de conectividade IP, permitindo a comunicação entre todos os acessos de uma determinada *VPN* e, não permitindo a comunicação com outros acessos não pertencentes àquela rede virtual formada.

Isso se dá por meio de uma tabela de roteamento *IP*, a qual determina a escola que fará parte desta rede privada, incluindo as políticas para o uso desta rede.

Já que as Escolas e o NTE receberam dos Programas de Governo os Laboratórios equipados, além do acesso, via ADSL ou via Satélite, dotados de um IP fixo, facilitando assim, a implantação da VPN proposta, e ainda, dispondo desses recursos, poderão solicitar um plano de roteamento IP à operadora de serviço, a fim de que seja implementada a rede privada virtual.

A criação da VPN possibilitará, por meio da técnica de tunelamento, a interligação das escolas geograficamente distantes, e, sugere-se assim, usar esta estrutura de rede para suporte técnico remoto, de forma que os técnicos que atendem estas escolas possam fazer uma prévia no atendimento técnico antes de se deslocarem até as escolas para compartilhar recursos de segurança, aplicando políticas para o controle de acesso.

Dessa forma, o que se pretende é, que as escolas possam elencar um nó concentrador (Prefeitura/Estado/NTE), os quais poderão ser providos recursos de autenticação, servidores

---

[17] Núcleo de Tecnologia Educacional, são unidades do PROINFO, vinculadas ao MEC e subordinadas às Secretarias de Educação. Tem a função de auxiliar as escolas em todas as fases de incorporação das tecnologias. <http://www.educacao.rs.gov.br/pse/html/nte.jsp?ACAO=acao1>

de conteúdos e filtros de acesso à Internet, em que a partir do ambiente escolar, os alunos tenham foco no conteúdo pedagógico e segurança para as atividades de ensino-aprendizagem, lançando mão de estrutura tecnológica, possibilitando ainda, que a mão de obra dos técnicos consiga prover a manutenção de tais recursos de forma centralizada ou remota.

4.2 VPN

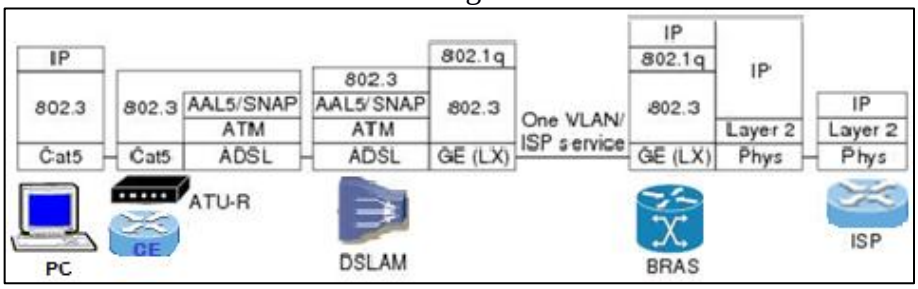
Como se sabe, a utilização dos recursos existentes para a criação da(s) VPN(s) que formará a proposta de rede para compartilhamento, autenticação e segurança, é feita a partir dos acessos ADSL e Satélite.

De acordo com o que foi explicado nos capítulos anteriores, a terminação dos acessos ADSL se dá nos equipamentos agregadores (BRAS).

Estes dispositivos encontram-se no núcleo da rede de um ISP e agregam as conexões dos DSLAM. É no BRAS que o ISP define as instâncias das sessões dos usuários, ou seja, além de agregar os circuitos, finalizando as sessões PPP, a partir de um ou mais dispositivos de acesso, é ele quem vai fornecer a conectividade entre a camada de enlace (camada 2 do modelo OSI), estabelecendo as rotas de tráfego para o acesso à camada 3 ou *backbone* do ISP.

A figura abaixo mostra um computador ligado a um *modem* (ATU-R) que chega a um terminador das linhas ADSLs, o DSLAM, conectado a um BRAS onde fornece o IP, passando por seu provedor ISP, observando-se então, o encapsulamento em cada etapa.

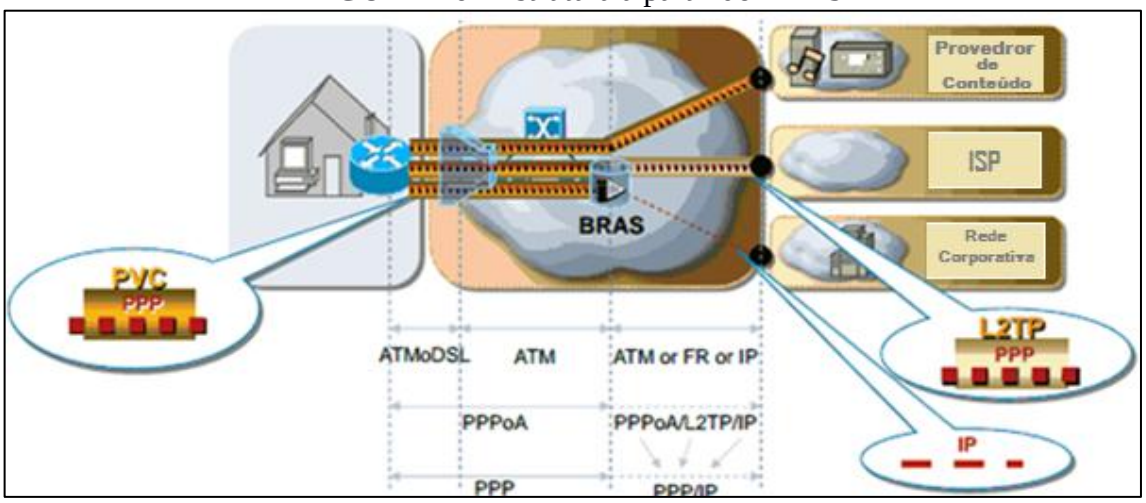
FIGURA 15 - DSLAM com VPNs configurados terminados em BRAS distintos.



Fonte: Elaborado pela autora, baseado no Henz, 2008. p.28

E também são apontadas as rotas de saída do acesso para a Internet, como mostra a figura abaixo:

FIGURA 16 - Estrutura a partir do BRAS



Fonte: Novaes, 2010. p.11.

Nesse sentido, se definirmos, os acessos ao chegarem no BRAS para que sigam com determinada identificação (*PVC* ou *VLAN*) por determinada rota que indique o destino comum, em todos os BRAS os quais finalizam suas sessões e, os roteadores do núcleo do ISP sejam capazes de reconhecer e encaminhar os pacotes de tais acessos em sua rede até um destino final, comum a todos eles, criamos o túnel virtual, e por conseguinte, a VPN.

A VPN será estabelecida a partir da estrutura existente, isto é, a escola conectada ao ISP por meio de uma conexão de banda larga (cabo ou DSL), ou Satélite. A composição da VPN se dá na interligação lógica dos pontos pré-determinados, no caso, as escolas e o ponto concentrador (Estado/Prefeitura/NTE), mediante o protocolo *Multi-Protocol Label Switching* ou, simplesmente, MPLS, que é um mecanismo de encaminhamento IP, os roteadores desta rede são compostos por FEC (*Foward Equivalence Class)***,** que é uma tabela de encaminhamento IP, é adicionado um cabeçalho, conhecido como label, e o pacote é encaminhado ao próximo roteador. Este cabeçalho é incluído no roteador de entrada *Label Edge Router* (LER), ou de borda, da rede MPLS, trafega no caminho (entre os nós de entrada e saída da rede MPLS) conhecido como *Label Switching Path* LSP passando pelos roteadores internos (LSRs) pré-configurados quando da criação da VPN. Estes labels são legíveis somente a roteadores pertencentes a esta rede, e quando o pacote chega ao último roteador de borda, LER, este irá retirar os labels para o encaminhamento IP ao seu destino, passando pelo concentrador.

E, para o *switch* ATM, o rótulo pode ser inserido no cabeçalho da camada de enlace nos campos de VCI ou VPI.

Segundo Oliveira (2012, p.43), o uso do MPLS em uma estrutura de rede VPN, além de oferecer maior agilidade no tráfego e tornar a rede mais segura, permite a integração de

qualquer tipo de rede, planos de endereçamento e roteamento, pois são os roteadores que representam o MPLS e são preparados para fazer a leitura dos rótulos e encaminhamento de pacotes, analisando e classificando o rótulo para direcionamento previamente definido, e assim, todo acesso deverá ser encaminhado por um *VR* (*Virtual Router*).

Nos roteadores *LER*, da rede MPLS do *backbone* do *ISP* são armazenados informações em uma *VRF Virtual Routing and Forwarding*, ou seja, uma tabela virtual de encaminhamento e roteamento do tráfego, que possibilita criar diferentes tabelas de roteamento lógicas, em um mesmo roteador físico, possibilitando a conexão de diversos pontos, por meio de equipamentos compartilhados, isolando a visualização da topologia da rede e, consequentemente, do tráfego de dados, os quais os usuários de uma VPN possuem acesso apenas a sites ou *hosts* dentro de uma mesma VPN.

4.3 SIMULAÇÃO

4.3.1 Cenário Criado

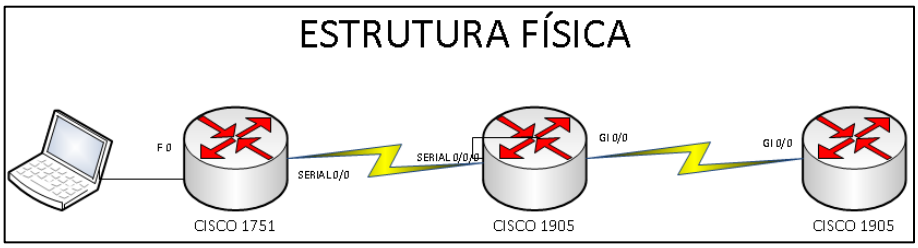
Para que se tivesse certeza da forma de aplicação e configuração da solução proposta nos ambientes existentes na rede da escola, usando PBLE e ou GESAC, foi criado um cenário utilizando equipamentos CISCO[18], simulando a estrutura necessária para compor a VPN, solução proposta por este trabalho.

A figura abaixo ilustra a estrutura física criada, na qual foram interligados 3 roteadores para representação básica dos equipamentos utilizados na solução. O CONCENTRADOR (Prefeitura/Estado/NTE), o acesso da ESCOLA e o BACKBONE da rede MPLS do ISP, representados por equipamentos CISCO1905, CISCO1751. Na estrutura criada, foram utilizados roteadores CISCO por conveniência, pois a estrutura ISP, que atende atualmente as Escolas de educação básica já se utiliza estes equipamentos, bem como o Projeto GESAC.

---

[18] **Equipamentos CISCO**: Dispositivos de ligação para redes de computadores, inclui roteadores ou routers, comutadores (switches) e centros (hubs). São equipamentos de código fechado, os quais foram mencionados e usados porque a estrutura ISP dispõe dos mesmos para atender as escolas.
< http://elmaxilab.com/pergunteme/ciencias/ask57738-O_que_e_cisco.html>

FIGURA 17 - Estrutura física criada simulando o uso da VPN



Fonte: Elaborada pela autora, 2014.

Para acesso e configuração dos roteadores, foi utilizado o Programa Minicon (software livre que permite acessar os roteadores via console).

Para configurar cada roteador, um notebook, dotado do software Minicon e de um cabo console foi conectado ao CPE.

Além da configuração padrão, para o roteador que simula o equipamento a ser disponibilizado na ESCOLA, conectado ao *modem* ADSL, foram inseridos os parâmetros de:

- -*hostname* ESCOLA (para reconhecimento local do elemento);
- interface Serial com o IP designado para aquele ponto, estipulado para a conectividade à VPN a ser formada;
- interface *fastethernet* com o IP de LAN para acesso da rede da escola, e por fim,
- a rota padrão, definição do primeiro salto do acesso.

A figura seguinte traz as configurações necessárias a serem aplicadas no Roteador de cada Escola:

FIGURA 18 - Configurações necessárias a serem aplicadas no roteador da escola

```
!
hostname ESCOLA
!
interface FastEthernet0
 description LAN_FNS2
 ip address 192.168.1.1 255.255.255.0
 speed auto
 full-duplex
!
interface Serial0
 description ESCOLA_PE
 bandwidth 2048
 ip address 10.10.2.2 255.255.255.252
 encapsulation ppp
 random-detect
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.2.1
no ip http server
```

Fonte: Elaborada pela autora, 2014.

Ao observarmos a configuração acima, pode-se notar que se trata de configuração básica de um roteador convencional, no qual é atribuído um IP para a rede local, e um IP para o acesso a uma rede remota, com uma rota que especifica para que lugar os pacotes devem ser encaminhados.

Neste caso, o acesso de última milha pode ser de qualquer tipo: ADSL ou Satélite, desde que suporte a conexão a um roteador.

A criação do túnel, realmente acontecerá, quando os pacotes do ponto remoto, no caso, a Escola, chegarem ao destino intermediário, ou seja, seu próximo salto.

É importante observar que na formação na VPN proposta, o IP de saída do roteador (10.10.2.2) não precisa ser um IP válido, uma vez que não sairá para a Internet de forma direta. Necessitará, portanto passar pelo concentrador, onde os servidores de acesso, conteúdo e Internet sugeridos estarão centralizados e, é a partir deste ponto, que a administração da rede pode ser exercida, ao ser criada uma gerência centralizada dos equipamentos/nós de rede.

E, quem faz o devido encaminhamento dos pacotes ao concentrador, responsável pela formação do túnel, é o roteador BACKBONE, que no cenário representa a nuvem do ISP.

No roteador que simula a estrutura ISP (*backbone*) foi configurada a VRF eat e associada a ela o rd 10:1111, dez é o numero da operadora e a subinterface 1111 (conexão lógica) é um número de identificação da VRF[19], quando criamos uma VRF, todo tráfego fica concentrado apenas naquela VRF, não sendo compartilhada com qualquer outra que seja. Um roteador pode ter várias VRFs, mas uma não enxerga a outra, isso é o que caracteriza a exclusividade da VRF, formando um túnel entre o concentrador e as escolas.

O rd é um identificador único dentro do *backbone ISP*, o mesmo é inserido, por meio da configuração do equipamento (roteador), diante do IPv4 fazendo com que as rotas IPv4 sejam únicas pela rede VPN MPLS, possibilitando aos usuários de diferentes VPNs o uso do mesmos endereços privados.

Em cada roteador localizado na estrutura MPLS do ISP encontramos as configurações da VPN, por meio da configuração da VRF e política de roteamento adotada.

No roteador que simula o equipamento a ser disponibilizado no *BACKBONE ISP*, conectado ao *CPE* da escola, e o *CPE* concentrador, foram inseridos os parâmetros de:

- *hostname* (para reconhecimento do local do elemento)
- vrf, definição do nome da vrf eat;

[19] VRF é um atributo designado em roteadores que suportem MPLS para realizar funções de uma rede privada. < http://www.rotadefault.com.br/vrf-em-roteadores-cisco/>

- rd, definição da identificação numérica para a operadora e para a vrf;
- *route-target*, importação e exportação da marcação dos pacotes na vrf;
- definição da sub-interface WAN da VRF;
- definição da Serial que dá acesso do BACKBONE para a escola;
- rota padrão, default para CPE concentrador; e por último,
- rota para rede da VRF para próximo salto.

A figura abaixo traz tais configurações aplicadas, e o apêndice A mostra toda a configuração aplicada aos respectivos roteadores.

FIGURA 19 - Configurações Aplicadas ao Backbone

```
!
hostname BACKBONE
!
ip vrf eat
rd 10:1000
route-target export 10:1111
route-target import 10:1111
!
interface GigabitEthernet0/0.1000
encapsulation dot1Q 1000
ip vrf forwarding eat
ip address 10.10.1.1 255.255.255.0
!
interface Serial0/0/0
ip vrf forwarding eat
ip address 10.10.2.1 255.255.255.252
encapsulation ppp
ip route vrf eat 0.0.0.0 0.0.0.0 10.10.1.2
ip route vrf eat 192.168.1.0 255.255.255.0 10.10.2.2
```

Fonte: Elaborada pela autora, 2014.

No roteador que simula o equipamento a ser disponibilizado no CONCENTRADOR, conectado ao roteador do BACKBONE, foram inseridos os parâmetros de:

- hostname (para reconhecimento do local do elemento);
- interface *fastethernet* com o IP de LAN para acesso da rede da escola;
- rota padrão, para Internet; e
- definição da rota da LAN para acesso à WAN.

A figura a seguir, traz as configurações do roteador R3 (concentrador), e o apêndice A, mostra toda a configuração aplicada neste roteador.

FIGURA 20 - Configurações do Roteador R3

```
hostname Concentrador
!
interface GigabitEthernet0/0.1000
 encapsulation dot1Q 1000
 ip address 10.10.1.2 255.255.255.252
!
interface GigabitEthernet0/0.2000
 encapsulation dot1Q 2000
 ip address 200.180.0.2 255.255.255.252
!
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 200.180.0.1
ip route 192.168.1.0 255.255.255.0 10.10.1.1
```

Fonte: Elaborada pela autora, 2014.

O cenário montado demonstra exatamente as configurações e as características necessárias que serão aplicadas na formação da rede VPN para as escolas, ou seja, um ponto concentrador deverá ser elencado, no qual servidores específicos sugeridos poderão estar instalados (pensou-se em servidor de acesso, conteúdo e segurança; no entanto, os NTEs poderão definir quais as necessidades e hierarquia serão aplicadas de forma a serem supridas as situações específicas para cada região) na qual um roteador R1 qualquer (similar ao *hostname* Concentrador) deve ser instalado e configurado; na escola, junto ao modem ADSL um CPE do tipo R2 qualquer (similar ao de *hostname* ESCOLA) deverá estar disponível e a estrutura definida junto ao ISP (que pode ser estabelecida por projeto do MEC nos moldes e experiência já adquirida com o GESAC e acompanhamento da ANATEL) de distribuição de IP's e VRF's deverá ser configurada, determinando a formação dos túneis.

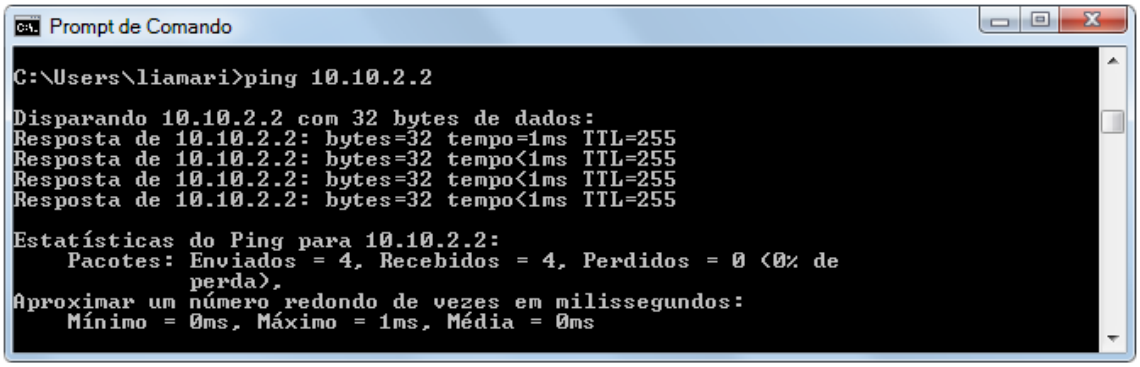
4.3.2 Simulação do ambiente de uma VPN

Ao montar o cenário, depois de configurados os equipamentos de rede, observam-se, abaixo, os testes.

Foi estabelecida para teste, a LAN com IP 192.168.1.0/24 para rede local da escola, neste endereçamento poderá alocar IPs, variando entre 192.168.1.2 a 192.168.1.254/24, para interligar os *hosts* (computadores) desta rede; e para a LAN do concentrador, foi definido o IP 172.16.1.1/24.

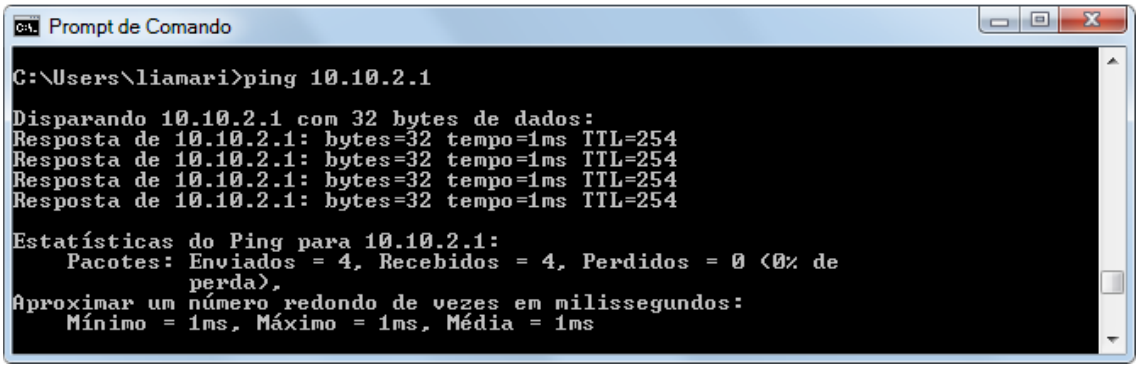
Na representação abaixo é mostrado um *ping* realizado a partir de um computador da escola até o *gateway* de saída (interface WAN do roteador ESCOLA):

- Passo 1- Considerando a rede local de origem, teste de conectividade entre roteadores.
  - IP DE ORIGEM: 192.168.1.1(LAN da escola)
  - IP DE DESTINO (ALVO): 10.10.2.2
  - OBJETIVO: TESTE DE CONECTIVIDADE ENTRE A LAN E A WAN.



Como se queria demonstrar, a partir da origem, a saída da rede local está assegurada.

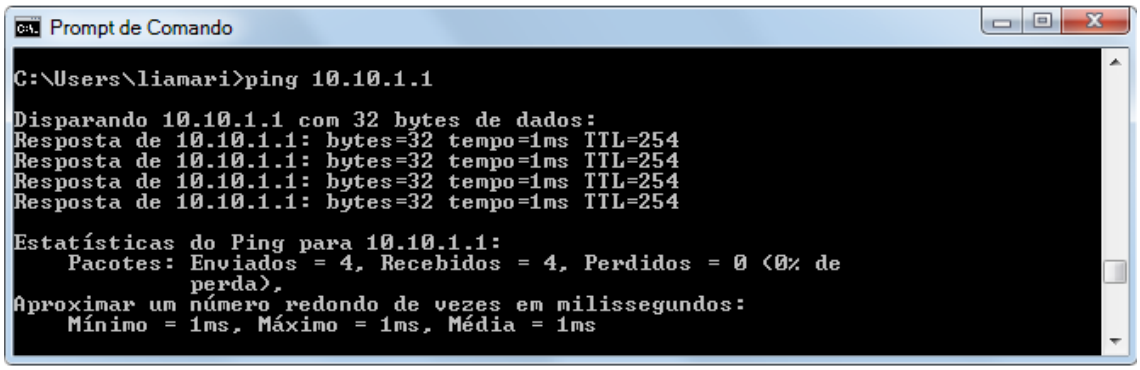
- Passo 2 - A partir da mesma origem, ou seja, de uma estação de trabalho da escola, buscou-se a conectividade com o próximo salto, ou seja, interface de entrada do *BACKBONE*:
  - IP DE ORIGEM: 192.168.1.1
  - IP DE DESTINO (ALVO): 10.10.2.1
  - OBJETIVO: TESTE DE CONECTIVIDADE ENTRE A LAN/WAN LOCAL E WAN REMOTA.



Completado: a partir da LAN, alcança-se o ISP.

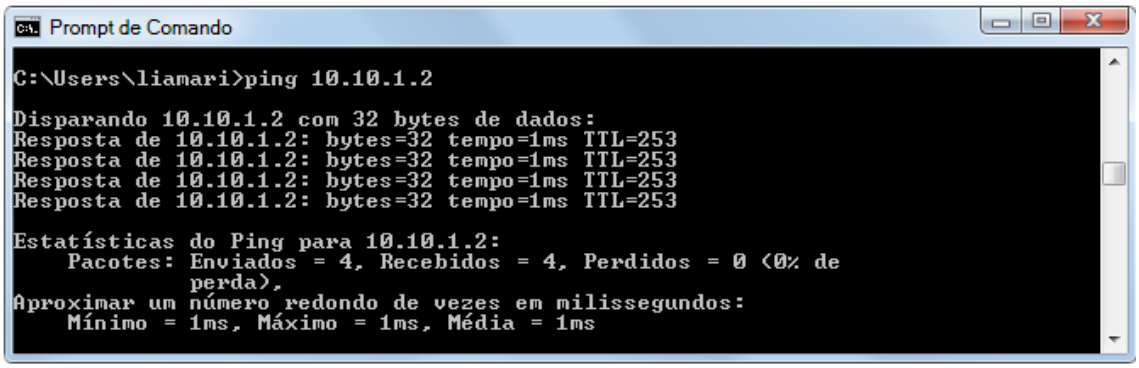
- Passo 3- A partir da origem, buscou-se a conectividade com o próximo salto, ou seja, interface de saída do BACKBONE:
  - IP DE ORIGEM: 192.168.1.1
  - IP DE DESTINO (ALVO): 10.10.1.1
  - OBJETIVO: TESTE DE CONECTIVIDADE ENTRE A LAN/WAN LOCAL E

WAN REMOTA.



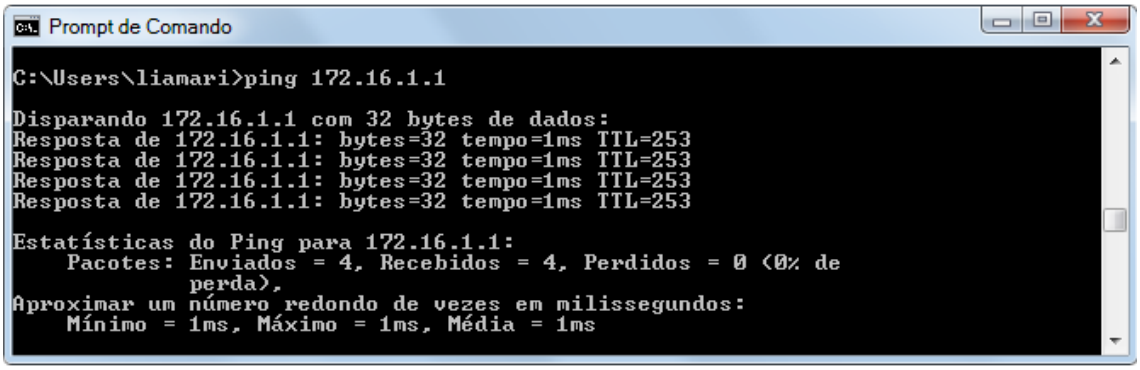
Completado: a partir da LAN, passa pela WAN do ISP.

- Passo 4 - A partir da origem buscou-se a conectividade com o próximo salto, ou seja, interface de entrada do concentrador (interface WAN):
  - IP DE ORIGEM: 192.168.1.1
  - IP DE DESTINO (ALVO): 10.10.1.2
  - OBJETIVO: TESTE DE CONECTIVIDADE ENTRE A WAN E A LAN E A INTERNET.



Completado: a partir da LAN de origem, entre a LAN/WAN local e WAN remota

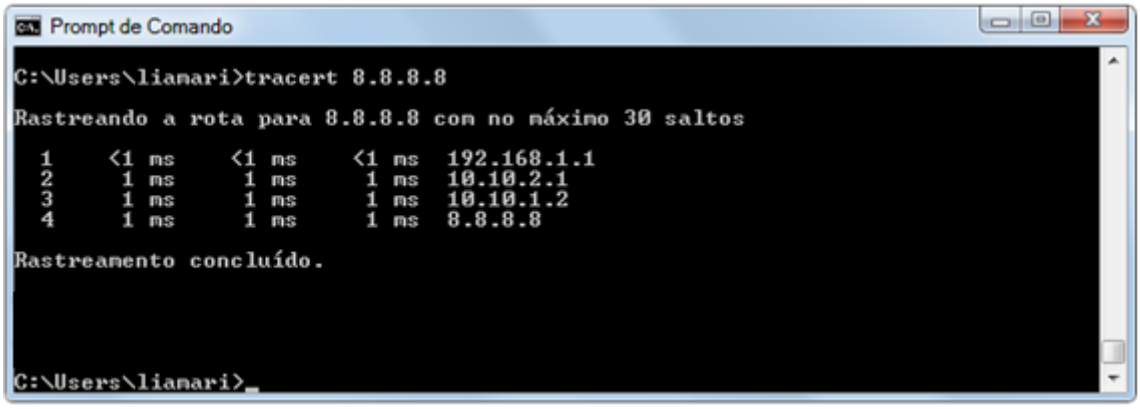
- Passo 5- A partir da origem, buscou-se a conectividade com o próximo salto, ou seja, LAN do concentrador:
  - IP DE ORIGEM: 192.168.1.1
  - IP DE DESTINO (ALVO): 172.168.1.1
  - OBJETIVO: TESTE DE CONECTIVIDADE ENTRE A LAN ESCOLA E LAN DO CONCENTRADOR.



Completado: a conexão ente as LANs, os roteadores, a partir da LAN da escola estão se comunicando, do ponto de origem ao destino.

Agora utilizando o comando *tracert*[20], montado dessa forma para simular o ambiente real, mostra-se que a partir da origem, ou seja, *host* na escola, os dados trafegam exatamente pelo túnel formado para acessar um endereço qualquer (no caso, foi escolhido o endereço 8.8.8.8, DNS Google) acompanhando-se o caminho por onde o pacote trafega (rede privada virtual).

- IP DE ORIGEM: 192.168.1.1
- IP DE DESTINO (ALVO): 8.8.8.8
- TRAJETO: 10.10.2.1 ENDEREÇO DA INTERFACE DE ENTRADA NO BACKBONE E 10.10.1.2 ENDEREÇO DA INTERFACE DE SAÍDA DO CONCENTRADOR
- OBJETIVO: VERIFICAR A ROTA POR ONDE PASSA O PACOTE.



Completado: conexão da LAN de origem com a Internet.

---

[20] Tracert é uma ferramenta para rastrear a rota, a qual acompanha a trajetória dos pacotes IPs na rede. < http://faqinformatica.com/como-utilizar-o-comando-traceroute-tracert-para-verificar-rotas-entre-equipamentos/>

4.3.3 Com mais de uma VPN

Para efeito de teste, foi configurada a VRF eat e, no mesmo roteador *BACKBONE* também foi configurada a VRF lia. Da mesma forma, foi associada a esta VRF o rd 10:7777, dez é o numero da operadora, que é a mesma operadora da eat e 7777 é um número de identificação da outra vrf (lia).

Portanto, somente as configurações do equipamento de *BACKBONE* foram alteradas, mantendo-se idênticas as configurações dos roteadores das pontas (ESCOLA e CONCENTRADOR).

```
!
ip vrf eat
 rd 10:1111
 route-target export 10:1111
 route-target import 10:1111
!
ip vrf lia
 rd 10:7777
 route-target export 10:7777
 route-target import 10:7777
!
interface Loopback0
 description GOOGLE
 ip address 8.8.8.8 255.255.255.255
!
interface Loopback777
 ip vrf forwarding lia
 ip address 10.10.10.10 255.255.255.255
!
interface Serial0/0
 ip vrf forwarding eat
 ip address 10.10.2.1 255.255.255.252
 encapsulation ppp
!
interface Serial0/1.100 point-to-point
 ip vrf forwarding eat
 ip address 10.10.1.1 255.255.255.252
 frame-relay interface-dlci 100
!
interface Serial0/1.200 point-to-point
 ip address 200.180.0.1 255.255.255.252
 frame-relay interface-dlci 200
!
ip route 0.0.0.0 0.0.0.0 200.180.0.2
ip route vrf eat 0.0.0.0 0.0.0.0 10.10.1.2
ip route vrf eat 192.168.2.0 255.255.255.0 10.10.2.2
```

É importante observar nesta configuração, que a rota *default* apontando para o IP 200.180.0.2, em um cenário real seria substituída por uma estrutura de NAT[21].

Para testar que a conectividade entre a VRF eat e a VRF lia não se processam, formando túneis distintos, tem-se inicialmente, a partir do *BACKBONE*:

```
BACKBONE#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
BACKBONE#ping 10.10.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
BACKBONE#
BACKBONE#ping vrf lia 10.10.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
BACKBONE#
```

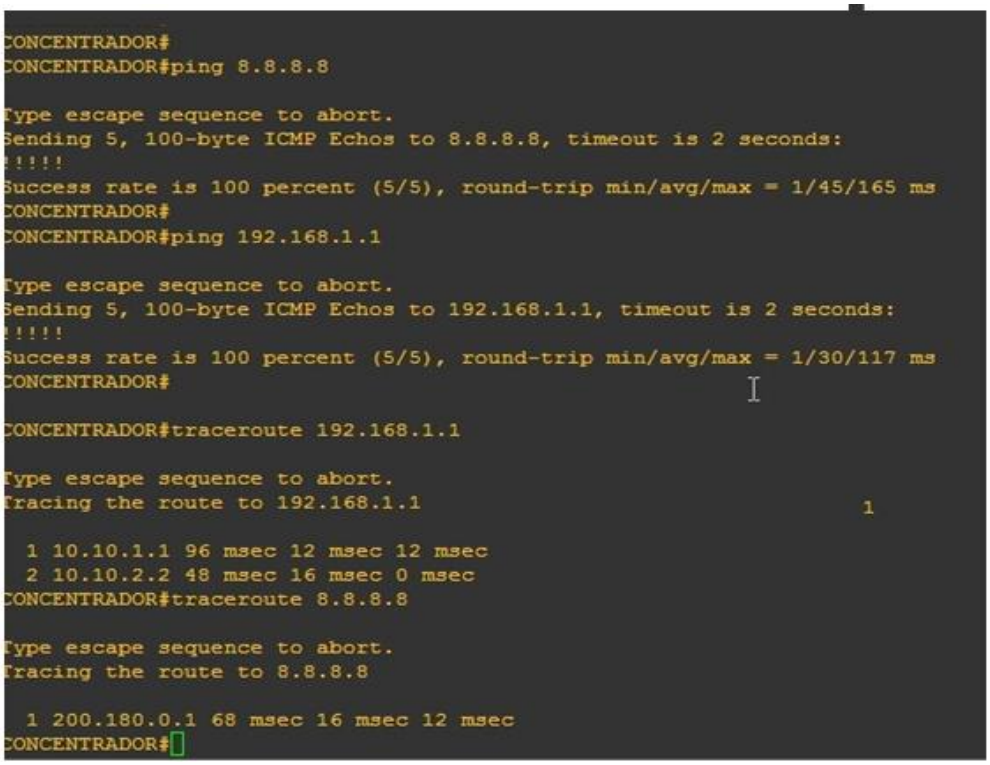
Demonstra-se que, a partir do equipamento de *BACKBONE*, ao se testar a conectividade (através do comando *ping*) ao endereço de DNS do Google, há sucesso.

De outra feita, um teste de conectividade ao endereço 10.10.10.10, obtém-se sucesso, confirmando-se a conectividade.

E, por fim, ao testarmos a conectividade, a partir do CONCENTRADOR e da ESCOLA para esta mesma rede, observa-se que:

[21] *NAT, Network Address Translation*, esta técnica faz com que um computador de uma rede interna tenha acesso à rede pública.

< http://pt.kioskea.net/contents/273-nat-network-address-translation-porta-e-encaminhamento-porta>



Os testes de conectividade, a partir do concentrador para o DNS do Google, são processados. Para a VRF lia não ocorrem, demonstrando que as VRF's são isoladas e não se comunicam. E, o *ping*, para o endereço 192.168.1.1 prova a conectividade. O comando *tracert*, para o endereço 192.168.1.1, na rede local da escola, acontece corretamente à conectividade, ou seja, a partir do CONCENTRADOR, com destino ao IP da rede local da escola, existem apenas os saltos para a interface de entrada no *BACKBONE* e depois, na entrada da WAN da escola. Mesmo que existissem, dentro do ISP, inúmeros saltos, a conexão seria direta, determinada pela formação do túnel VPN de nível 2, estabelecida pela construção de VRFs e MPLS.

```
ESCOLA#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/24/88 ms
ESCOLA#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/17/64 ms
ESCOLA#tra
ESCOLA#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.10.2.1 28 msec 16 msec 0 msec
  2 10.10.1.2 16 msec 0 msec 0 msec
  3 200.180.0.1 16 msec 0 msec 0 msec
ESCOLA#traceroute 172.16.1.1

Type escape sequence to abort.
Tracing the route to 172.16.1.1

  1 10.10.2.1 32 msec 0 msec 0 msec
  2 10.10.1.2 112 msec 0 msec 0 msec
ESCOLA#ping 10.10.10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
ESCOLA#
```

Assim sendo, a partir então da ESCOLA, foram realizados testes de conexão através do comando *ping* e, observou-se que os equipamentos se comunicam. O comando *tracert* demonstrou o caminho percorrido dentro da VRF criada, uma vez que os saltos acontecem, apontando para os IP’s de interface daquele elemento, bem como é possível o acesso ao IP de LAN do CONCENTRADOR (172.16.1.1), mas não é possível o acesso à rede da VRF lia.

Isso foi feito para demonstrar que uma estrutura de VRF não interfere na outra, mesmo estando no mesmo nó de rede ou com IP’s da mesma rede, ou seja, mantendo uma VPN opaca à outra.

5 CONCLUSÃO

O presente trabalho se dedicou a relatar que as escolas de ensino básico da grande Florianópolis, são dotadas de acessos ADSL ou Satélite para comunicação com a Internet. Sendo assim, mediante este estudo, com base na fundamentação teórica, nas simulações e na visita à escola e, sob o ponto de vista das telecomunicações, buscou-se entender como estes serviços tecnologicamente existem e funcionam.

Muito embora o acesso à Internet tenha inúmeras vantagens, um acesso aberto traz consigo diversos ônus, como dispersão de conteúdos, falta de segurança na navegação, dificuldades de uso ou acesso, por questões de operação da rede ou dos equipamentos.

Este estudo se propôs a oferecer uma alternativa de padronização, interligação da rede da escola, mediante os recursos do Programa Banda Larga nas Escolas e, como forma de consolidar o aprendizado adquirido durante o curso de Sistemas em Telecomunicações, pelo estudo da formação e aplicação prática de técnicas de acesso VPN, definindo como configurar os equipamentos da estrutura proposta para o seu funcionamento, por meio de uma rede de compartilhamento de recursos geograficamente distribuída.

Dessa forma, entende-se que a criação da VPN possibilitará, mediante a técnica de tunelamento, a interligação das escolas geograficamente distantes, e assim, usar esta estrutura de rede para suporte técnico remoto, de forma que os técnicos (NTE) poderão fazer uma prévia no atendimento, antes de deslocamento de profissional habilitado para o local, pois este cenário possibilitará a criação de uma estrutura de gerenciamento de redes centralizada, através do uso da VPN que oferecerá a possibilidade de acesso aos recursos de informática, usando o túnel por caminho direto de comunicação com a entidade remota, e ainda, em pontos concentradores, estabelecer recursos de segurança, aplicando políticas para o controle de acesso e/ou outros, como conteúdos que se façam necessários para cada região, conteúdos estes, que podem estar disponibilizados diretamente em servidor no ponto de concentração ou dispersos e acessíveis, via Internet, de forma focada e segura para quem objetiva usar tais recursos.

Com o auxílio da fundamentação teórica e das simulações executadas e demonstradas, pôde-se comprovar a eficácia da aplicação da técnica como meio de interligação e comunicação entre as escolas, sem grandes incrementos de custos, apenas com adequação de projeto, nos moldes atualmente utilizados pelo governo com o programa GESAC que já tem por base, definidos, pontos de concentração terrestres, que fazem a etapa de segurança, de encaminhamento para os serviços de conteúdo e acesso a Internet, padronizando as

configurações dos equipamentos de telecomunicações a serem instalados, e definindo uma política de roteamento como se fossem em uma grande rede local.

Logo, este trabalho se vale como fonte de análise e possibilidade para apontar o uso das técnicas de acesso VPN, como revisão das especificações da ANATEL para o PNBE, de forma a cumprir a revisão do programa há cada 3 anos.

Ainda, do ponto de vista tecnológico e de aprendizado, foram usadas de forma prática, ferramentas fornecidas durante o Curso Superior de Sistemas de Telecomunicações do Instituto Federal de Santa Catarina, principalmente das disciplinas de redes de computadores, essenciais para o entendimento dos tópicos de funcionamento e criação de redes, tanto locais como geograficamente distribuídas, protocolos e roteamento de uma forma geral.

Unindo assim, conhecimento adquiridos nos estudos tecnológicos, fundamentação teórica, disposição em se fazer a tecnologia servir de instrumento na melhoria, principalmente da qualidade do processo ensino-aprendizagem foi que se compôs este trabalho.

6 SUGESTÃO PARA TRABALHOS FUTUROS

Entre outros possíveis estudos e definições de como se compor a estrutura de informática – servidores de acesso, conteúdo, VOIP a ser disponibilizada nos concentradores e suas políticas de acesso; possível interligação dos pontos remotos (escolas) a estrutura concentradora e de segurança já existente no sistema GESAC; sugere-se também, prover a estrutura de VPN através do uso de roteadores de código aberto, que possam vir a possibilitar o desenvolvimento de produtos que agreguem funcionalidades de formação de redes, não só do tipo VPN, mas também, para virtualização e computação nas nuvens.[22]

[22] Computação na nuvem é a possibilidade de acessar arquivos e executar diferentes tarefas pela internet. Quer dizer, você não precisa instalar aplicativos no seu computador para tudo, pois pode acessar diferentes serviços online para fazer o que precisa, já que os dados não se encontram em um computador específico, mas sim em uma rede.
<http://www.tecmundo.com.br/computacao-em-nuvem/738-o-que-e-computacao-em-nuvens-.htm>

REFERÊNCIAS

ANATEL. **Lei Geral de Telecomunicações (LGT) – Lei 9.472.** Disponível em: < http://legislacao.anatel.gov.br/leis/2-lei-9472> Acesso em: 23 set. 2013.

BARCELAR, Ricardo Rodrigues. **Como funciona o sinal *DSL***. Disponível em: <http://www.ricardobarcelar.com.br/arquivos/como_funciona_adsl.pdf> Acesso em : 25 set. 2014

BRASIL. Ministério da Educação e do Desporto. **Programa Banda larga nas Escolas**. Disponível em: <http://portal.mec.gov.br/index.php?option=com_content&view=article&id=15808:programa-banda-larga-nas-escolas&catid=193:seed-educacao-a-distancia#content> Acesso em 06 jun. 2013.

GESAC. **Cartilha GESAC**. 2ª ed. Ministério das Comunicações, 2010. Disponível em: <http://www.institutoembratel.org.br/projetos/projetoGesac/swf/documentos/guias/CARTILHA_GESAC_02.pdf> Acesso em: 03 set. 2014.

COSTA, Jefferson, **Apostila de Redes de Computadores**. Disponível em <http://www.jeffersoncosta.com.br/redes.pdf> Acesso em: 21 jun. 2013.

FAGUNDES, Eduardo Mayer. **ATM – Asynchronous Transfer Mode**. Disponível em <http://efagundes.com/openclass_networking/wp-content/uploads/Slide101.jpg> Acesso em 18 ago. 2014.

GRUSZYNSKI, André. **Mecanismo Funcional Escalável para Contabilização de uso de Serviços Residenciais em Rede de Acesso em Banda Larga Utilizando Tecnologia *ADSL***. Disponível em: < http://repositorio.unb.br/bitstream/10482/2462/1/2008_AndreGruszynski.pdf> Acesso em 27 nov. 2014.

GILHERME, Paulo. **O que é ping**. 2012, TECMUNDO. Disponível em: <http://www.tecmundo.com.br/internet/715-o-que-e-ping-.htm> Acesso em: 23 jun.14

HAFFERMANN, Leonardo. **Segmentação de Redes com VLAN**. 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Haffermann%20-%20Artigo.pdf>Acesso em: 20 set. 2014.

HENZ, Leandro. **Proposta e Implementação de Arquitetura para Identificação Física e Lógica de Acessos Banda Larga Utilizando Tecnologia ADSL**. Publicação: PPGENE.DM-057/2008 Brasília/DF: Julho, 2008.

MONTEIRO, Sandro de Castro. **Modelo de Avaliação da Capacidade da Rede de Acesso Metálica para o provimento de Serviços Suportados pela Tecnologia ADSL**. Dissertação (Mestrado Profissional em Engenharia Elétrica) Universidade de Brasília. 2007. 78f.

NASCIMENTO, J.Q. **Satélites para acesso à banda larga**. Em debate 02 mai. 2012. Disponível em: <http://www.teleco.com.br/emdebate/quadros13.asp> Acesso em: 28 out. 2013.

NETO, Benedito Medeiros. **Pensar BH/Política Social, Programa GESAC, Inclusão Social direito de todos.** 2009. Disponível em:
< www.antoniomiranda.com.br/ciencia_informacao/pensar.pdf> Acesso em 26 set. 2014.

NOVAES, Bruno. **Comunidade de Suporte CISCO**, 2010. Disponível em: <https://supportforums.cisco.com/sites/default/files/legacy/8/6/9/96968-CSC_BNG%20Workshop.pdf> Acesso em 13 ago. 2014.

NTE. **Núcleos de tecnologia Educacional**, 1998. Disponível em: <http://www.sed.sc.gov.br/educadores/nucleos-de-tecnologia-educacional-nte> Acesso em: 19 ago.2012.

NUNES, Paulo. **Conceito de *Ethernet***, 2007. Disponível em: <http://www.knoow.net/ciencinformtelec/informatica/ethernet.htm> Acesso em 04 ago. 2014.

OLIVEIRA, Ednei Nunes de. **A Utilização dos Laboratórios de Informática do PROINFO em Escolas de Dourados–MS**. Dissertação (Mestrado em Engenharia de Produção) Programa de Pós-Graduação em Engenharia de Produção, UFSC, Florianópolis, 2001.92f.

OLIVEIRA, José Mário; LINS, Rafael Dueire; Mendonça, Roberto. **Redes MPLS**: **Fundamentos e Aplicações**; Editora Brasport, 2012. 223 p.

PROINFO. **Programa Nacional de Informática na Educação**. 1995. Disponível em: <http://www.fnde.gov.br/programas/programa-nacional-de-tecnologia-educacional-proinfo> Acesso em 25 jun.2013

SARLO LINO, d.S Virtual Private Network. **Aprenda a construir redes privadas virtuais em plataforma Linux e Windows**. Novatec, 2003.

SIGNIFICADOS. **Significados de Índice de Desenvolvimento Humano**. 2014. Disponível em <http://www.significados.com.br/idh/> Acesso em 19 ago. 2014.

SILVA,L.R. **Tecnologias de Acesso**. 2013. Disponível em: <http://leandrodriguesilva.wordpress.com/temas-sugeridos/tecnologias-de-acesso/> Acesso em: 07 mai. 20014.

SOARES, Luiz Fernando Gomes; LEMOS Guido; COLCHER Sérgio. **Redes de Computadores das LANs, WANs e Wans as Redes ATM**. Elsevier, 1995. 705 p.

TANENBAUM, Andrew. S. **Redes de Computadores**. Rio de Janeiro. Ed. Elsevier, 2003. 945 p.

VALENTE, Paulo. **Virtual Private Networks**. Leiria: SIEMENS, 2001, 76 slides, color. Acompanha texto. Acesso em 06 abr. 2013

APÊNDICE

A.1 - Configurando do roteador Cisco 1700, representando A ESCOLA.

```
ESCOLA#sh running-config
Building configuration...

Current configuration : 2055 bytes
!
! Last configuration change at 19:47:31 UTC Thu Sep 4 2014
! NVRAM config last updated at 19:48:01 UTC Thu Sep 4 2014
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ESCOLA
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable password cisco
!
ip cef
!
interface FastEthernet0
 description LAN_FNS2
 ip address 192.168.1.1 255.255.255.0
 speed auto
 full-duplex
!
interface Serial0
 description ESCOLA_PE
 bandwidth 2048
 ip address 10.10.2.2 255.255.255.252
 encapsulation ppp
 random-detect
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.2.1
no ip http server
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
end
```

A.2 - Configurando o roteador Cisco 1900, representando o BACKBONE ISP.

```
BACKBONE#sh running-config
Building configuration...

Current configuration : 1669 bytes
Last configuration change at 10:46:35 UTC Mon Nov 17 2014
! NVRAM config last updated at 10:12:41 UTC Mon Nov 17 2014
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
     no service password-encryption
!
hostname BACKBONE
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$BBaW$q9hkmjzKsTk/uVtA6kK8H/
!
     no aaa new-model
     !
     no ipv6 cef
     ip source-route
     ip cef
     !
     !
     ip vrf lia
      rd 10:7777
      route-target export 10:7777
      route-target import 10:7777
     !
     ip vrf eat
      rd 10:1111
      route-target export 10:1111
      route-target import 10:1111
     !
     multilink bundle-name authenticated
     !
     !
     license udi pid CISCO1905/K9 sn FTX1626Y0AV
     !
     interface Loopback0
      ip address 8.8.8.8 255.255.255.255
     !
     interface Loopback22
      ip vrf forwarding lia
      ip address 10.10.1.1 255.255.255.252
     !
     interface GigabitEthernet0/0
```

```
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.1000
 encapsulation dot1Q 1000
 ip vrf forwarding eat
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0.2000
 encapsulation dot1Q 2000
 ip address 200.180.0.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip vrf forwarding eat
 ip address 10.10.2.1 255.255.255.252
 encapsulation ppp
 no fair-queue
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 200.180.0.2
ip route vrf eat 0.0.0.0 0.0.0.0 10.10.1.2
ip route vrf eat 192.168.1.0 255.255.255.0 10.10.2.2
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
end
```

A3 Configurando o roteador Cisco 1900 representando o concentrador:

```
Router#sh run
Building configuration...

Current configuration : 1932 bytes
!
! Last configuration change at 10:30:56 UTC Mon Nov 17 2014
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Concentrador
!
boot-start-marker
boot-end-marker
!
enable password sn2
!
no aaa new-model
!
no ipv6 cef
ip source-route
ip cef
!
multilink bundle-name authenticated
!
license udi pid CISCO1905BR/K9 sn TSP1802ACMB
!
!
username sn2 password 0 sn2
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.1000
 encapsulation dot1Q 1000
 ip address 10.10.1.2 255.255.255.252
!
interface GigabitEthernet0/0.2000
 encapsulation dot1Q 2000
 ip address 200.180.0.2 255.255.255.252
!
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
```

```
interface Serial0/0/0
 no ip address
 clock rate 2000000

ip route 0.0.0.0 0.0.0.0 200.180.0.1
ip route 192.168.1.0 255.255.255.0 10.10.1.1
!
control-plane
!
!
line con 0
 password sn2
line aux 0
line vty 0 4
 password sn2
 login
!
scheduler allocate 20000 1000
end

Router#
```